Stratus 3.3

Administration Manual

A guide to the Administrative Interface

videoNEXT®

Stratus 3.3 Administration Manual
A guide to the Administrative Interface
Edition 3

Copyright © 2002-2013 videoNEXT Federal, Inc. Security Synchronized. All Rights Reserved Worldwide

No part of this document may be copied or reproduced in any form or by any means (print, photographed, sent via electronic mail, sent via postal service or by such means) without the prior written consent of videoNEXT Federal, Inc. dba, videoNEXT.

videoNEXT makes no warranties with respect to this document and disclaims any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. videoNEXT reserves the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

Trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective owners.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED ON AN AS-IS BASIS.

VIDEONEXT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS.

IN NO EVENT SHALL VIDEONEXT BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

1. Introduction **1**

2. Planning Your Stratus System **3**
2.1. Deployment Planning Considerations 3
2.2. Install and Upgrade Procedures Outline 6
2.3. Multi-Node Stratus Installations 7
2.4. Storage System Planning and Configuration outline 7
2.5. Time Considerations 7

3. Quick Start - Initial System Configuration **9**
3.1. Logging In to the Control Panel 9
3.2. Multi-Node Configuration Management 11
3.3. Stratus License Installation 14
3.4. Manage Storage and Storage Consumers 16
3.4.1. Manage Storage Volumes 16
3.4.2. Manage Storage Consumers 19
3.5. Configuring Cameras 20

4. Advanced System Configuration **23**
4.1. Cameras 23
4.1.1. The General Tab 23
4.1.2. The Source Tab 25
4.1.3. The Image Tab 26
4.1.4. The PTZ tab 27
4.1.5. Camera Motion Detection 27
4.1.6. The Storage Tab 31
4.1.7. The Schedule Tab 31
4.1.8. Analytics Configuration 32
4.1.9. Camera GEO-Calibration 34
4.1.10. The Set Tab 37
4.1.11. The Audit Tab 38
4.1.12. Email on Events 38
4.2. Configuring DNS, NAT and Firewall 40
4.3. The Audit Log 40
4.4. Users and Roles and Management 41
4.4.1. User Access and Permissions 42
4.4.2. Resources and Sets Management 43
4.4.3. Role Management 44
4.4.4. User Management 44
4.5. Storage Policies Management 45
4.6. Configure Event Handling 48
4.7. Configure Sensors 51
4.8. Media Export 52
4.9. Configure v-MX (Video Wall) 53
4.10. Configure v-AC (Access Control) 57
4.11. Schedule Manager 58
4.11.1. The Schedule 59
4.11.2. Postures 60
4.11.3. Scheduling a Posture Timecard. 62
4.12. Configure vCrypt 64

5. Suggestions **67**
5.1. Recommendations on Client Station platforms 67

6. Troubleshooting **69**
6.1. How to Identify and Classify the issue 69

6.2. Issues with Client Station 69
6.3. Issues with Stratus Server 70
6.3.1. Camera does not retrieve video 70
6.3.2. Camera PTZ does not work 72
6.4. Documenting Software Issues and Getting Support 72

A. Analytics **75**
A.1. Types of Tracker Rules 75
A.2. VCA Tracker Configuration 76
A.2.1. VCA - Adding and Editing Zones 77
A.2.2. VCA - Adding and Editing Lines. 80
A.2.3. VCA - Channel Settings 81
A.2.4. VCA - Classification 83
A.2.5. VCA - Calibration 84
A.3. OV Tracker Configuration 85
A.3.1. OV - Adding and Editing Zones 86
A.3.2. OV - Adding and Editing Lines. 88
A.3.3. OV - Adding and Editing Multilines. 90
A.3.4. OV - View Settings 93

B. Video Codecs, Transmission Protocols and their Effective Usage **95**

C. Detailed Steps **97**
C.1. Stratus software Installation in details 97
C.1.1. Prepare OS (Linux only) 97
C.1.2. CentOS Linux 101
C.2. Upgrade from Stratus 2.7.1 104
C.3. Software Upgrade 104
C.3.1. Software Upgrade Through SOS Account 104
C.3.2. Software Upgrade 105
C.3.3. Remote Software Upgrade 105
C.4. Using “S.O.S.” Account for system administration/recovery (Linux only) 107
C.5. Adding Storage 108
C.6. Importing and Exporting CSV camera lists 108

D. Device Support **111**
D.1. Supported Video Cameras 111
D.2. Supported Relay / Sensors 112

E. Support **113**

F. Release Notes Stratus 3.3 **115**

G. Revision History **121**

Introduction

The videoNEXT team is proud to present Stratus™ 3.3.0, the software solution that will improve and simplify the operation and management of your security systems.

Stratus allows you to build and grow your security system based on your existing IT infrastructure.

Stratus, an open, standards-based software solution that works with almost any IP, digital, or analog camera including HD and mega pixel; runs on any Intel or compatible server (now on the Mac); and uses your existing security and data infrastructure in new and powerful ways. With thousands of systems currently installed and a rock solid reputation for no downtime during critical installations, Stratus is a proven security technology for today and beyond.

Stratus provides the easiest and most scalable Physical Security Information Management (PSIM) solution available today. This, combined with full policy-level administration, flexible Storage Volume Manager and the renowned Frame Rate Decimation feature gets you the most capable and scalable surveillance and security tool ever developed.

Most importantly, the Stratus software platform leverages a classical IT approach to video and sensor content management:

- CAPTURE- data from an infinite quantity of cameras, access control, sensors, ground based radar, point of sale, etc.
- ORGANIZE- data into a single, intelligent workable database.
- STORE- data in commercially available storage arrays, in accordance with enterprise archival policies.
- DISPLAY- video and sensor data in an intuitive graphical user interface to all credentialed users via; web browser, or wireless device.

Planning Your Stratus System

This chapter will provide you with an introduction into the most common situations Stratus Administrators face when installing, maintaining, or troubleshooting Security System software.

After you read this chapter you will have a conceptual understanding of how to:

- Install and/or upgrade Stratus software
- Plan your Stratus installation
- Configure and maintain cameras and sensors
- Administer Users' Access and Permissions
- Utilize other options and services within Stratus
- Ensure optimal operation

Please see *Chapter 4, Advanced System Configuration* for further reading and detailed instructions.

2.1. Deployment Planning Considerations

One of the most important things to keep in mind when planning your Security System deployment is that you have to plan your installation for future growth to make sure you are effectively using your initial investment as your Security System expands.

Please review the simple Stratus deployment schema below:

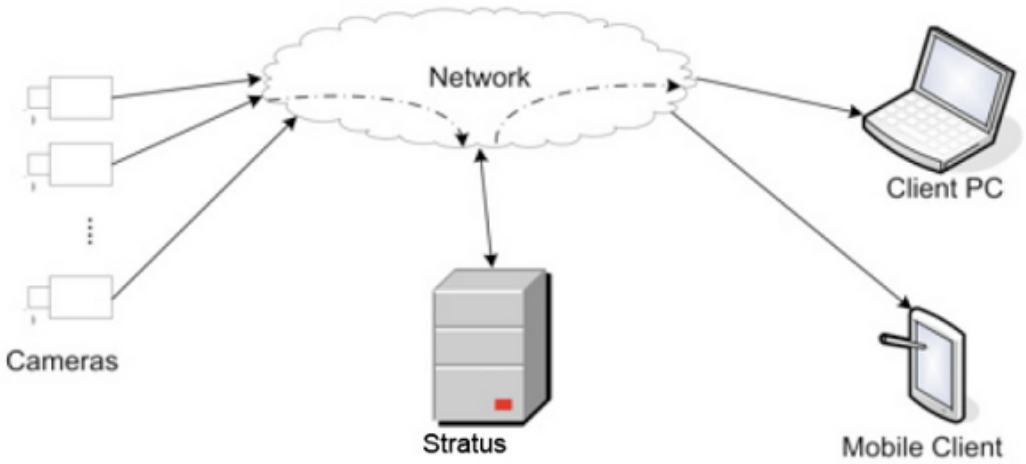


Figure 2.1. A Simple Deployment

The setup is very simple. It interconnects media producers (cameras) to consumers (clients) through a network, where a Stratus Server provides the middle-point. The server manages cameras, provides video-recording and media analysis, and leverages multiple camera manufacturers' specifics into a uniform user experience for Clients.

As the number of video feeds grows this setup will easily scale by extending the network infrastructure, and a linear expansion of the number of Stratus servers. The user experience will be kept uniform regardless of how many cameras and Stratus servers your setup will have. Stratus software is specifically accommodated to span multiple servers with no need to require users to log in to individual servers.

The total number of Clients registered in the system is not limited, and Stratus will be able to support tens and hundreds of simultaneously connected and actively working users as long as your network infrastructure is sized properly to accommodate such a load. Still, the “simple” setup has one important limiting factor: the number of video feeds that can simultaneously be viewed is limited by the power of the CPU and graphics card available on the client's computer.

In a more advanced setup as depicted in the schema below, you will see how Stratus overcomes this limitation and grows beyond it:

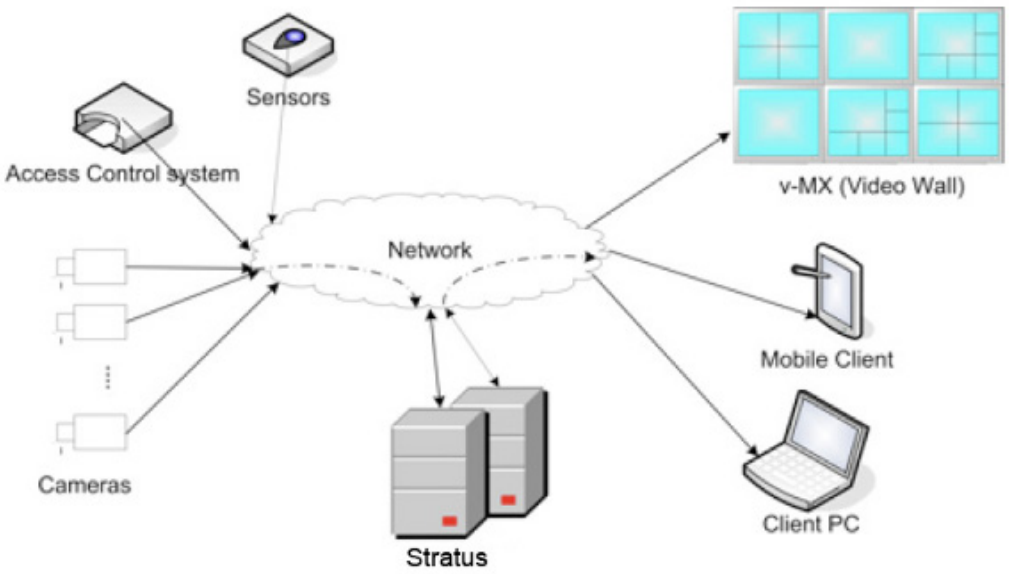


Figure 2.2. A More Complicated Deployment

In this diagram the “Video Wall” concept comes into use. The video wall allows for the creating of multi-monitor / multi-view viewing solutions with generic inexpensive video monitors and COTS (Common Off The Shelf) computers. Video Walls can be shared between Clients, who use the extended User Interface features to control Video Walls, while retaining their ability to work with video on their personal computers. This solution not only extends simultaneous video visualizations capabilities, but it improves the reliability and survivability for critical applications.

Another scenario that is depicted on the schema is an integration with Access Control Systems and Sensors. Here, Stratus becomes a focal point of Signal Processing and Control by keeping the user experience uniform in receiving Alerts and controlling such devices as Door Readers, Keypads, etc.

It is important to carefully examine the following areas of the Digital Security System design in order to determine how best to set up your system.

1. Data Acquisition devices (Cameras/Sensors/Access Control Systems/etc..)
   - If you are doing a new installation - investing in natively IP-enabled devices may be a little bit pricier, but will benefit you by achieving a faster/cheaper roll out using standard network infrastructures and less expensive maintenance on network-enabled devices down the road.
   - If you are retrofitting an existing system - you might consider keeping legacy analog data acquisition devices (like cameras and sensors), while adding analog-to-digital converters, which, again, may give you a faster/cheaper roll out and less expensive maintenance in the long run.
2. Network Infrastructure
   - Media streams (Video and Sound) are heavy on transmission and storage by definition, so your network should have sufficient capacity for proper bandwidth handling.

- Network designs should allow for the growth, as experience shows that Security Systems tend to grow bigger with time.
- Reasonable consideration should be given to the reliability and network security due to the nature of the data that will be transmitted and processed.

3. Data Storage
   - Storage is the largest potential bottleneck for system performance. Just as the network needs to be able to handle the load of video streams you are planning on using, the storage must also be able to write as fast while still maintaining enough addition resources for archive to be viewed again.
   - Storage internal to the hardware may be used for systems where long retention time is not needed.
   - As demand for longer retention time grows - externally attached storage should be considered for its scalability, reliability and manageability.
   - For both speed and reliability, some form of RAID is strongly recommended.
4. Accurate Time
   - An often overlooked aspect is the necessity for accurate time.
   - The Stratus system uses its own time to know when to archive video. It is important that the system has an accurate source for time that will not drift. Such a source should be external, either an accessible NTP server or some attached device (such as GPS) with an accurate clock.
   - It is also mandatory that all nodes and all clients are synced with the main Stratus server. In 3.3, Stratus now comes with NTP enabled (on Linux), so all nodes and clients can be synchronized to the main server.
5. Data Processing
   - The primary constraint with Stratus is the speed that video archive can be written to a disk. After that, however, processing power is the next concern.
   - There are two major components that rely on processing power: the number of cameras, and the number of clients.
   - Analytics provides a heavy data processing load. As such, it is recommended that your system has a spare CPU-core per Analytics channel you are expecting to run. For instance, if you are trying to run Analytics on three cameras, you will need a minimum of a four-core processor.
6. Server Hardware
   - Stratus processes data on Servers, and Common-Off-The-Shelf (COTS) hardware from most leading vendors.
   - Consideration should be given to overall system reliability and maintainability. This aspect depends on the hardware provider and on the set of management tools which will be installed.
   - If the installation consists of multiple processing Nodes (Servers) - you may consider rack-mountable hardware to decrease the installation footprint.
7. Client Platforms

- Stratus client software requires a standard browser on any Windows or MAC OS X to operate.
- Dependencies include Java Runtime 1.6 update 22 and Adobe Flash 9 (or later revisions).
- GEO-mapping capabilities require optional Google Earth browser plug-in to operate in 3D mode.
- The number of simultaneously visualized video feeds depends mostly on client computer CPU power and on a reasonably powerful (mid-class) video adapter.
- If simultaneous display of more then 8-12 videos is expected - consideration should be given to either deploying a v-MX (Video-Wall) Stratus option (preferred) or to boost the CPU on the viewing station above the average of “office PC” class.

8. Scaling the system
   - The Stratus software automatically binds multiple Nodes to form the Stratus Security Domain, where resources are presented to the Administrators and End Users in one logical cluster.
   - As your system grows - you can scale close to linear by adding more Stratus Nodes to accommodate system expansion.
   - Each Stratus node will support a number of cameras (and other sensors) per node depending on the resolution. For instance, on a single mid-range server with internal storage configured with RAID 5, up to 45 video streams each with a 4Mb/s bitrate were able to run on a single server
   - The Stratus licensing schema is flexible to accept any number of processing nodes you might need, i.e. it does not charge for additional processing node[s], but it does change for the number of sensors and for the enabled processing options.
   - The Storage System will have to grow as you expand your security system. Each new Stratus-node will require its own storage, so as you scale the system and add additional nodes you will also need to expand the storage.
   - The v-MX (Video Wall) Stratus option should be seriously considered for installation with above-average requirements on the number of simultaneous video-feeds displayed.

2.2. Install and Upgrade Procedures Outline

Stratus 3.3 software works under Red Hat Enterprise Linux OS 5.6 and APPLE Mac OS X 10.6 and newer.

The software installation itself is a very straightforward process (described in greater details below in *Appendix C, Detailed Steps*), while a careful look should be given to the preparation and planning that precedes it.

Before installation on any platform, the disk system has to be prepared to accept the software through the creation of a specified disk layout. On Linux, a number of dependency packages should be installed. videoNEXT provides a special “kick-start” scenario to simplify and automate the installation process.

Once the prerequisites are met the Stratus software package will configure OS components (such as the database and web server) to have the proper settings. No additional configuration will be needed.

To upgrade from a previous versions of Stratus, a special set of upgrade scripts is embedded into the software package to facilitate the automated configuration and content migration. Please refer to *Section C.2, “Upgrade from Stratus 2.7.1”* inside this document for the upgrade procedure from a prior major Stratus release 2.6.

2.3. Multi-Node Stratus Installations

The Stratus installation is easily scalable by adding additional Nodes (servers running Stratus software). Once such nodes are added, the compound system will behave as a single compound set of resources which is called Stratus Security Domain. The User will be unaware that the Stratus installation is comprised of multiple nodes and no special actions will be needed for accessing the resources.

Stratus Nodes perform a “handshake” with each other in multi-node configurations and this process is fully automatic. You will find more details in *Section 3.2, “Multi-Node Configuration Management”*

2.4. Storage System Planning and Configuration outline

Storage configuration is one of the most important tasks to be done when a Stratus system gets installed. Reliable, properly sized hardware and properly configured options are the keys to success.

Stratus automatically discovers and manages the storage for you, but it is still the Administrator's responsibility to assign the storage resources for management.

The newly installed Stratus system will not have any storage pre-configured, so before you proceed any further, please consider the following:

- Internal server storage should be considered a good economical option for entry-level systems when the media archival rate is moderate. Such storage options tend to have good performance only with relatively insignificant concurrency levels
- As your number of simultaneously recorded media-streams grows - you need to consider using cache-controllers (with “write-back” option and battery memory backup) and storage drives designed for high levels of concurrency (like SAS and enterprise class or SATA-2 drives with NCQ option)
- Various RAID options (internal storage with RAID controller or external RAID solutions) should be seriously considered when media storage reliability is of concern and no “shadow backup” of some sort is an option (which is true in most cases)
- When deciding on RAID level close attention should be given to RAID data write performance for massive concurrent write operations. It is important that the write performance is good enough when the RAID is degraded, not just when optimal. Once a non-fatal disk failure occurs, RAID may substantially degrade the write performance and disrupt media archival. This increased load makes secondary (fatal) disk failures very common, for such situations with RAID levels 3/4/5.
- RAID-6 is one of the best options, as it degrades very gracefully when a drive failure occurs, and allows up to two drives to fail without fatal data loss.
- Using “spare drives” with automated fail-over should be considered routine when working with RAID.

Please refer to *Chapter 5, Suggestions*for more information on the best practices when planning system storage.

2.5. Time Considerations

The Stratus server keeps track of data based on the time the data is generated. Without accurate time, and time that is synchronized between nodes and clients, discrepancies can occur.

For example, if a node is one hour behind the main Stratus server, when the main server looks for video from the node, that video will be off by an hour. Worse, if the main server looks for archive from five seconds in the past, the node will be trying to access video from 59 minutes in the future (from its perspective). This can lead to a false conclusion that the node is not archiving video.

To help prevent this scenario, Stratus 3.3 for Linux has a built in Network Time Protocol (NTP) server that other nodes and clients can synchronize with. This should help prevent most major problems that can arise, however it is still recommended to have this main server be synchronized with a more accurate source.

An internal clock on a server or consumer-grade computer can “drift” several seconds over the course of a day. Synchronizing the system with an outside NTP server is recommended. If a WAN network connection is available and NTP is not blocked, Stratus 3.3 should automatically synchronize with Red hat time servers (if on Linux) or Mac time servers (if on Mac). If the Stratus is on an isolated network, a local time server or GPS-based time server is recommended.

Quick Start - Initial System Configuration

Note

The Stratus software should already be installed, and it should be possible to access the software from the recommended browsers.

Please refer to *Appendix C, Detailed Steps* for details on the installation specifics for your particular OS.

This section will detail how to accomplish configuring the different pieces needed to get a bare-minimum installation operational. Later sections will detail specific configuration steps.

We will cover how to:

- Log in to the Stratus system.
- Configure the Stratus Nodes (separate servers in cluster forming Stratus Security Domain) - see *Section 3.2, “Multi-Node Configuration Management”*.
- Configure the Storage (as Cameras will not have a place to store video, otherwise) - see *Section 3.4, “Manage Storage and Storage Consumers”*.
- Configure the Cameras - see *Section 4.1, “Cameras”*.
- Configure the Credentials (so that your Users will use the system) - see *Section 4.4, “Users and Roles and Management”*.

When you finish the above steps you should be able to use Stratus for the most basic scenarios.

3.1. Logging In to the Control Panel

Once installed, the Stratus system is accessible through the regular browser. Please open it by pointing your browser to the Stratus “master” domain name or IP address. You should see a login screen similar to the one shown in *Figure 3.1, “Login Screen”*.

Figure 3.1. Login Screen

You have the option to choose Spanish, Russian or Arabic, as well as the default of English, as the system language.

Note

Changing the language will change the character set as well as the read-direction (i.e. right-to-left versus left-to-right) for your session on the server.

This manual will assume a left-to-right reading orientation.

The Administrator's default login name is “admin” and default password is “topse”. For security reasons, please make sure you change it when you finish with the system's initial configuration (see *Section 4.4, “Users and Roles and Management”*).

The next screen will show system warnings or errors. This will include messages about cameras being in a "broken" state, time-synchronization, and storage being offline or critical. If this is the first time you are logging in to the system, it will show warnings about the system license, the lack of storage, and the lack of cameras.

Since the “admin” user by default has access to any User Interface, the next screen will be the “Interface Selector”, where you are given the option between “Control Panel” or “Operator Matrix”. You will need to choose "Control Panel" to continue with the system administration.

You should now be logged in to the system and in the Control Panel interface.

3.2. Multi-Node Configuration Management

The maximum number of devices Stratus can operate is limited by the hardware performance of the server Stratus is installed on. Usually this limitation is caused by reaching the write-capacity of the storage volumes. For this reason, Stratus is scalable to span multiple servers.

There are two states for a Stratus server: a Master or a Node. There can be only one Master, and it is in charge of zero or more Nodes. Each node is responsible for the devices on that node, and for communicating event, status, health, and other information back to the Master server. For this reason, the Master server will have a higher load than the Nodes. As a security system grows, you will want to have fewer cameras (proportionally) hosted on the Master server; if the security system grows large enough, you will even want to remove cameras from the Master entirely.

After installing Stratus on a server, you must activate Stratus. This activation menu will give you an option to make the server a [M]aster or a [N]ode. More information can be found in *Section C.1, “Stratus software Installation in details”*. Once you have chosen the role of a server (either Master or Node), you will have to reinstall that server to change the servers role from a Master to a Node or vise-versa.

Stratus maintains a special “s_master” alias as a statically configured DNS entry (in /etc/hosts). This alias is managed through the "sos" account (see *Section C.4, “Using “S.O.S.” Account for system administration/recovery (Linux only)”*). This DNS entry is what defines who the Master server is, and which provides a stable name for “master server” in the Stratus Security Domain. This alias is maintained on every node in the Domain and should be tightly monitored to point to the proper network IP address of the “master server”.

Important

If this alias is changed (e.g. because the Master has changed, or changed IP addresses), the Stratus software should always be restarted. If the Master's IP has changed, all nodes will need to be restarted.

The “s_master” alias exists even in single-server Stratus installations and must always point to the correct node IP address. This alias is managed through the “sos” account (*Section C.4, “Using “S.O.S.” Account for system administration/recovery (Linux only)”*) and Stratus software should always be restarted if “s_master” alias gets changed.

Stratus automates the multi-node systems’ configuration by a special “handshake” procedure between “node” server and “master” server. This handshake is performed every time the Stratus software is started, guaranteeing that the node always operates alongside its proper master.

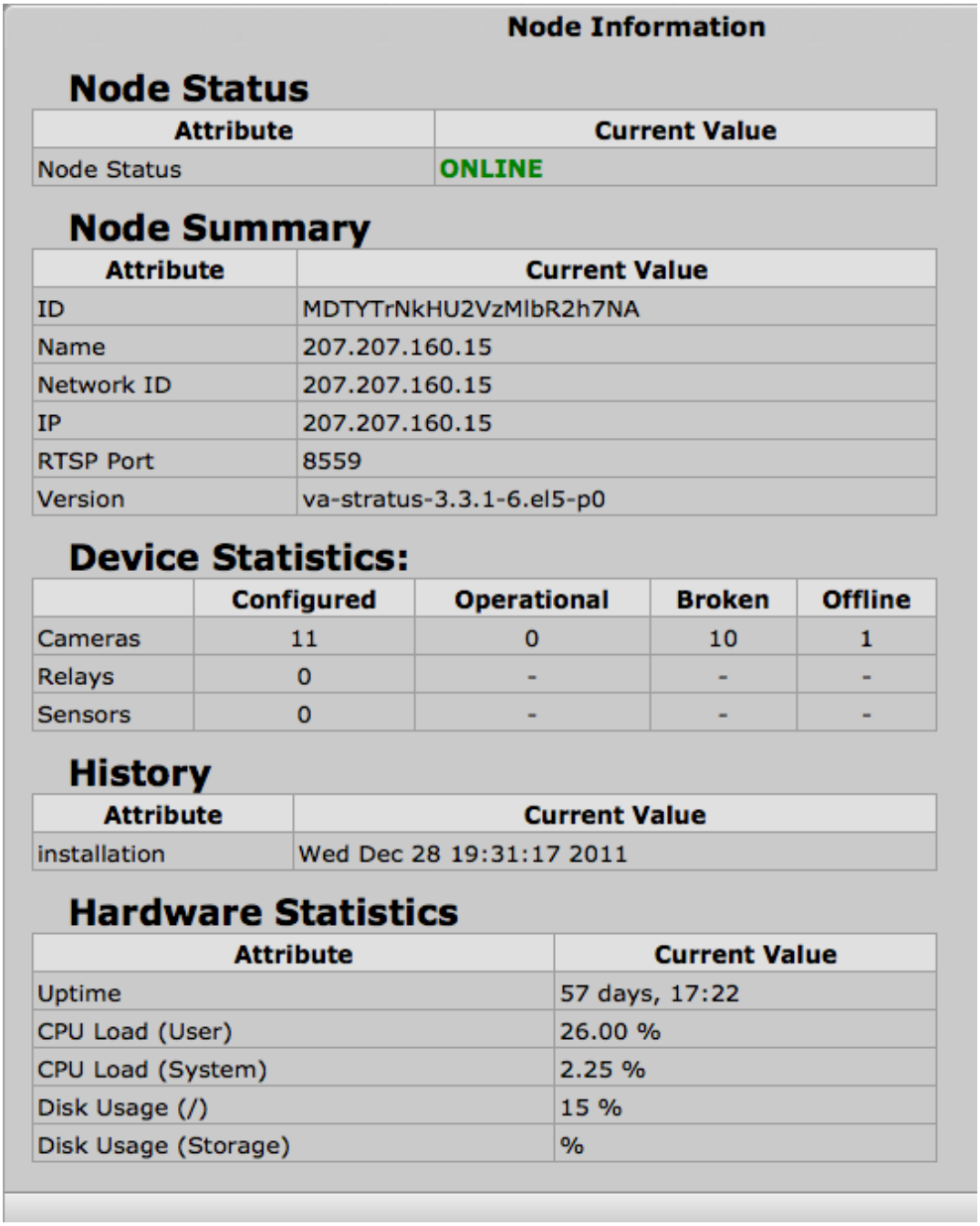
Newly recognized nodes are placed into the “Nodes” list in the left side of Admin Interface Control Panel. The Node information provided here allows the user to review the Node's operational status (online/offline/broken) and to identify devices managed by this particular node. Normally, device management is performed outside of the Node context, but this “Node Content” screen allows the review of devices currently allocated to the node, if needed.

Note

When adding a new device, Stratus will automatically try to place the device on the server with the least devices already configured. This is a simple method to provide load-balancing across servers, however it does not take in to account the bandwidth or other resources (such as processing power if running Analytics) that server is utilizing. Some thought should be given to how best to distribute cameras between servers based on the load you expect to encounter.

If the Node becomes non-operational, the “Node Information” screen will identify the node as broken. It will then be able to be removed from the Stratus Security Domain. It is impossible (intentionally or accidentally) to remove an operational Stratus Node from the Stratus Security Domain, as a safeguard against possible errors. If you must remove the Stratus Node from the Master, the system should be powered down first, and then it can be removed from the “Node Information” screen.

To summarize, nodes’ management in Stratus is mostly automated and is performed in the background to minimize the potential for errors.



Node Information

Node Status

Attribute	Current Value
Node Status	ONLINE

Node Summary

Attribute	Current Value
ID	MDTYTrNkHU2VzMlbR2h7NA
Name	207.207.160.15
Network ID	207.207.160.15
IP	207.207.160.15
RTSP Port	8559
Version	va-stratus-3.3.1-6.el5-p0

Device Statistics:

	Configured	Operational	Broken	Offline
Cameras	11	0	10	1
Relays	0	-	-	-
Sensors	0	-	-	-

History

Attribute	Current Value
installation	Wed Dec 28 19:31:17 2011

Hardware Statistics

Attribute	Current Value
Uptime	57 days, 17:22
CPU Load (User)	26.00 %
CPU Load (System)	2.25 %
Disk Usage (/)	15 %
Disk Usage (Storage)	%

Snapshot with a two-node system' Admin Interface opened, where "master" node is automatically loaded into the right side of the screen for device management purposes.

Figure 3.2. A two node system

From the “Control Panel” you can access the Nodes by clicking on “Nodes” on the left-side panel. To view information about the Nodes, Click the IP address for the master, followed by “Node Information”. Here is a snapshot of a two-node system in the Control Panel, with one server expanded:

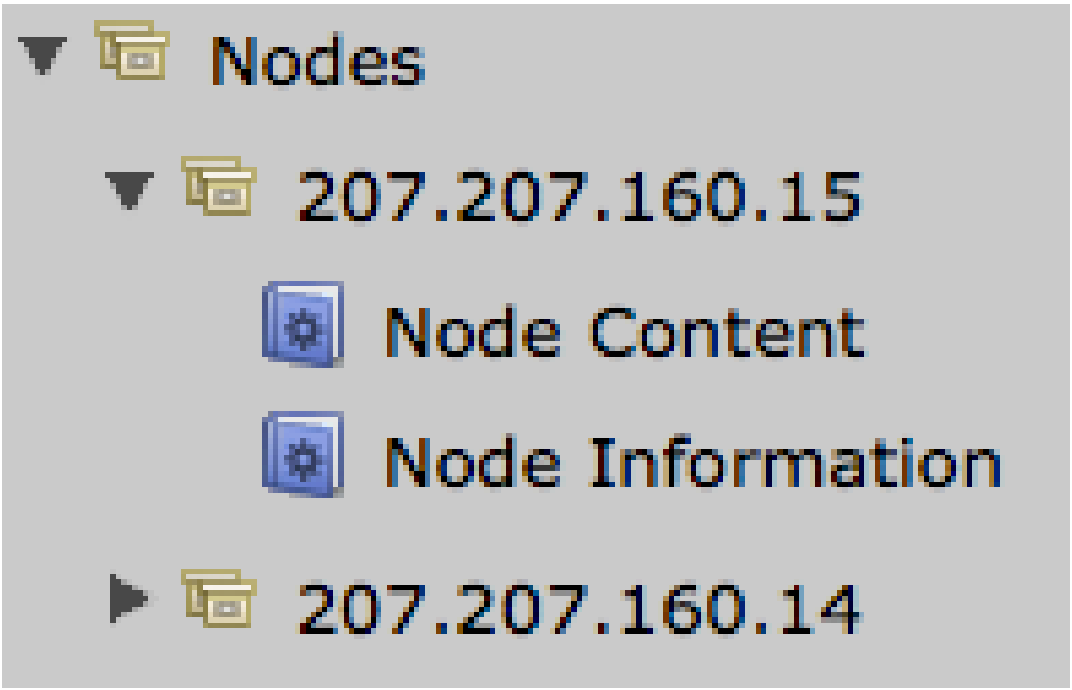
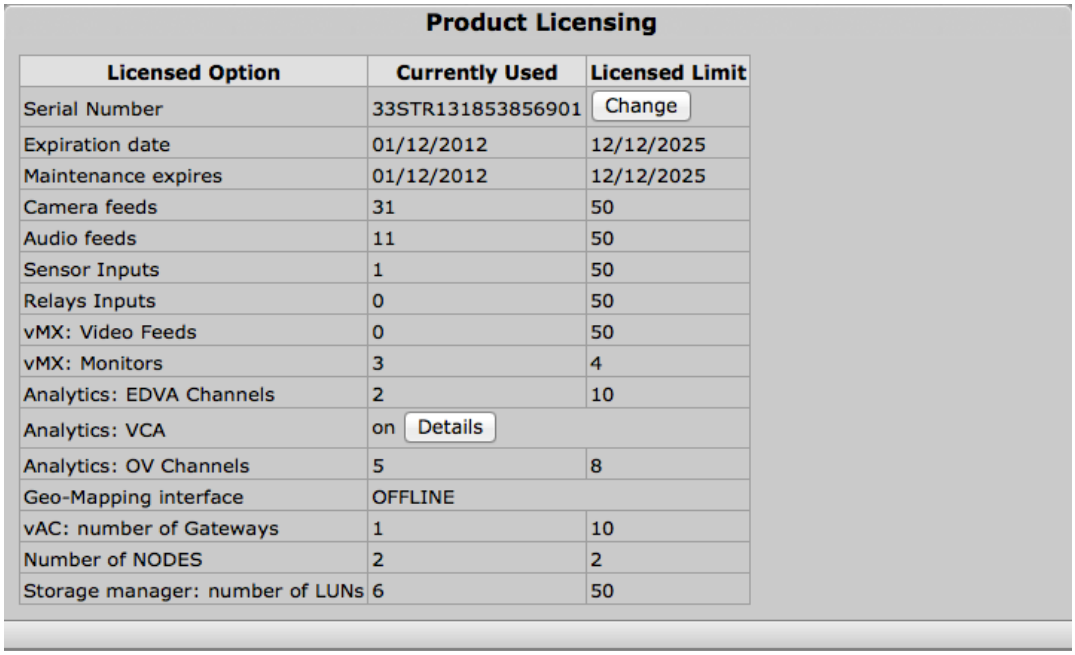


Figure 3.3. Node Content and Information

3.3. Stratus License Installation

This section explains how to install a new license on to the Stratus system.

1. Use web-browser to login as “admin”
2. Open ”Admin GUI”
3. Open Licensing page (General -> Licensing)
4. Here you can see if the system already has license installed (and Serial Number) and/or you can install/change the license by clicking on “Change” button, which will ask you for Serial Number and will perform a new license activation automatically if you have a connection to the Internet.
5. If Stratus software is not able to establish communications with the videoNEXT licensing server, it will prompt you to perform “offline activation”.
6. The most likely reason for you to be redirected into offline activation is that your system is installed on a network segregated from the Internet. In this case, you will have to perform limited information transfer by the means other then direct Internet connection in order to activate the license (see below).



Product Licensing

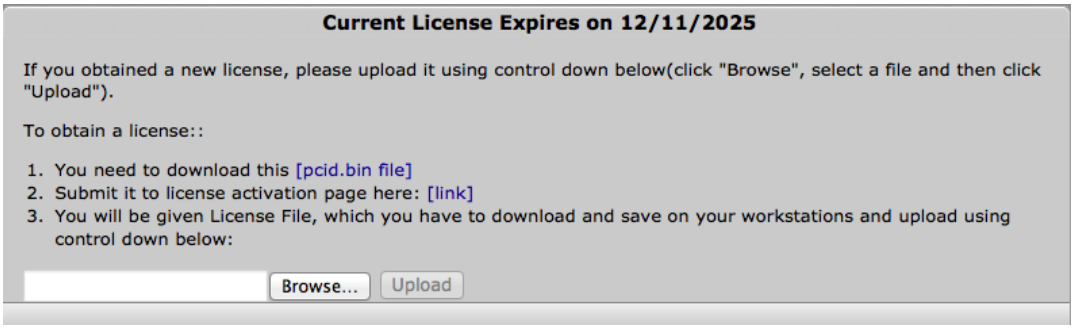
Licensed Option	Currently Used	Licensed Limit
Serial Number	33STR131853856901 Change	
Expiration date	01/12/2012	12/12/2025
Maintenance expires	01/12/2012	12/12/2025
Camera feeds	31	50
Audio feeds	11	50
Sensor Inputs	1	50
Relays Inputs	0	50
vMX: Video Feeds	0	50
vMX: Monitors	3	4
Analytics: EDVA Channels	2	10
Analytics: VCA	on Details	
Analytics: OV Channels	5	8
Geo-Mapping interface	OFFLINE	
vAC: number of Gateways	1	10
Number of NODES	2	2
Storage manager: number of LUNs	6	50

Figure 3.4. Licensing

Offline Activation:

1. You will be asked to download “pcid.bin” file

   See screenshot for details:



Current License Expires on 12/11/2025

If you obtained a new license, please upload it using control down below(click "Browse", select a file and then click "Upload").

To obtain a license::

1. You need to download this [pcid.bin file]
2. Submit it to license activation page here: [link]
3. You will be given License File, which you have to download and save on your workstations and upload using control down below:

Browse... Upload

Figure 3.5. PCID.bin

2. Click on [link] in the offline license activation page to open the license activation page, *http://licenses.videonext.com/SLM/upload_pcid.php*. You might need to write down the URL and manually enter it on another computer with Internet access.

3. Once you have access to offline licenses activation page, please upload your PCID file when prompted and you will be forwarded to the new page with “download license” link. Save this file on the media you can transfer to the location with access to the Stratus system.

4. Return to Stratus offline license activation page and click on “Install license”.

5. Click on "Browse...", find your license file saved on Desktop (example: 33STR131825381312.lic), and upload the license into your Stratus system.

6. Chose General/Licensing from left menu and check license details. At this time the system should report a valid license, and show you what you license is good for.

3.4. Manage Storage and Storage Consumers

Stratus's Storage System is in constant motion and balance:

- Cameras and audio-devices record media to the Storage. They are the Consumers.
- The Storage Manager constantly monitors Storage Providers (Volumes) to ensure Consumers always have accessible and healthy storage.
- Policy enforcement tools monitor Storage for sufficient space reserve to store content and for “hard limits” such as “maximum time to store”.

Storage volume limits and health monitoring are, for the most part, automatic and provide the best operating conditions for this particular configuration.

Consumers are assigned to Storage Policies, which prescribe the “hard” and “soft” limits, as well as retention policies. Stratus comes with several predefined policies, the default allows for fully automated management based on the Storage Space available and (in the case of video) the presence of motion in the video.

Of the next three subsections, it is mandatory to perform the procedure described in *Section 3.4.1, “Manage Storage Volumes”*. The other two procedures are optional and allow you to take finer control of the system, but they are not essential for normal operations.

Note

Please be sure to review *Section 4.6, “Configure Event Handling”*, which affects the storage consumption and should be taken into consideration.

3.4.1. Manage Storage Volumes

To use the “Storage Manager” screen, you will have to select “Settings”/ “Storage Manager” in the left panel of Admin Interface.

The “Storage Manager” screen will be loaded. This screen shows the Storage System configuration and status for all the Nodes in the Stratus Security Domain. From here, you can manage the storage on any Node.

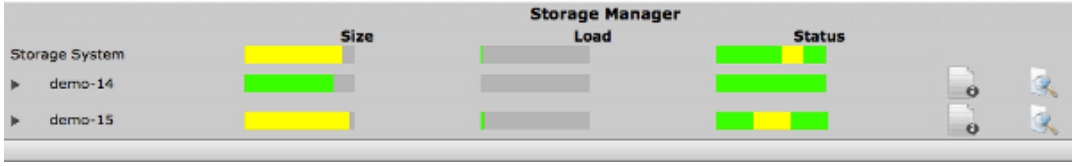


Figure 3.6. Storage Overview

The Size, Load, and Status columns in the above picture provide graphical summaries for the entire Storage System as well as summaries for individual Nodes. In this example, the “demo15” Node has three volumes, two are ONLINE, while the second one is in the SUSPENDED state, so it will not accept any new media at this time.

Note

Typically, columns should be in the “green” zone, but it is quite normal for individual volumes to reach the “yellow” or “red” state in the “size” column, while the Node and/or entire Storage System are expected to stay in the “green”.

Note

Stratus is capable of automatically discovering any type of storage device that is presented as a standard “local” storage device. This includes ATA, and SCSI and iSCSI, SAN if it is properly configured and using the appropriate OS utilities.

Double-clicking on the “Settings” icon results in the icon changing to the “ASSIGNED” state (folder with green up-arrow). Another click will change the storage to an “OFFLINE” setting (cogwheel with grey down-arrow). Another mouse clicks on the status icon will change it to “ONLINE” as pictured below.

Figure 3.7. Storage Status - Offline

Figure 3.8. Storage Status - Online

The Volume is also assigned for the automated management by Stratus and is in an “ONLINE” state. Stratus will automatically take the actions needed to healthfully maintain this volume and to accept and store the media data.

va-0003
Time Level Note
2011-02-22 16:24:25 INFO Full -(ONLINE)-> Online
2011-02-22 16:24:25 INFO Volume is OK (problem Tight is cleared)
2011-02-22 16:23:55 INFO Online -(ONLINE)-> Full
2011-02-22 16:23:55 WARNDISK FULL: 0/1;
2011-02-22 16:23:55 INFO Mount -(ONLINE)-> Online
2011-02-22 16:23:55 INFO Volume is mounted successfully
2011-02-22 16:23:55 INFO scanning for space usage
2011-02-22 16:23:55 INFO Start -(ONLINE)-> Mount
2011-02-22 16:23:55 INFO Check FS is completed with code=0
2011-02-22 16:23:55 INFO Chek FS consistency (fsck)
2011-02-22 16:23:55 INFO Offline -(ONLINE)-> Start
2011-02-22 16:21:50 INFO Stop -(OFFLINE)-> Offline
2011-02-22 16:21:45 INFO unmount
2011-02-22 16:21:45 INFO Online -(OFFLINE)-> Stop
2011-02-22 16:21:45 INFO [add] SUCCESS: ID=6bc33ddf-2a98-4d87-85c0-f26d4673eb15 [va-0003] is assigned to wheels
2011-02-22 16:21:45 INFO [add] SUCCESS: ID=6bc33ddf-2a98-4d87-85c0-f26d4673eb15 is UNUSED now

Figure 3.9. Storage Health

Note

Stratus will maintain and present for review the most recent log of actions relevant to a particular Volume, Node, or overall Storage system. It is accessible to the Admin with a mouse click on the “Log view” icon (the folder with an “i”). In the picture above, the Volume Log shows the entries that are a result of the changing a Storage Volume from the "Unused" state to the "Online" state.

The scenario described above demonstrates how to recognize and add a new Volume to the Storage System. Other types of Storage Volume Management operations are similar in method and execution and include:

- Temporarily suspending “write” operations to particular Volume (useful when it is needed to perform maintenance without getting Volume unmounted)
- Taking a Volume OFFLINE for maintenance (with full unmount)
- Removing a Volume from the Storage System (it will have to be brought OFFLINE, then DEMOTED, then REMOVED)

3.4.2. Manage Storage Consumers

Once your Storage system is configured and the Storage Policy is established, the Storage Consumers Management is the next step. In essence, you assign your Storage Consumers (cameras) to use a particular Storage Policy.

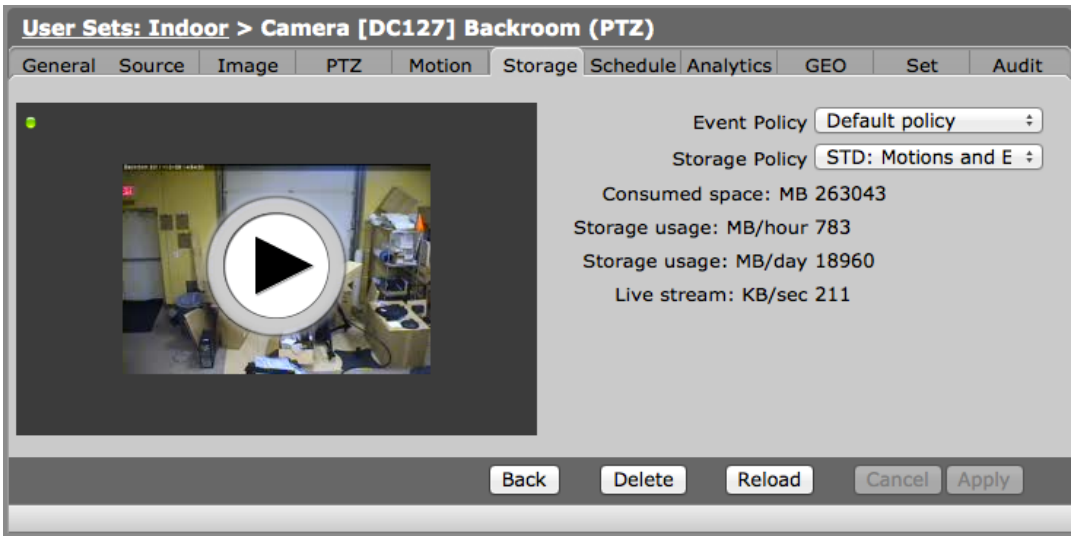


Figure 3.10. Cameras are storage consumers

One method is to load the individual camera configurations and assign the Storage Policy from the drop-down list. This method works best when you work with relatively few cameras.

Another method is to load the “Cam Config” page from the “Devices” menu and load a matrix of cameras’ settings. It is possible to select a Storage Policy in the first column and propagate it to all the cameras in the row by using the “+” on the left of drop-down.

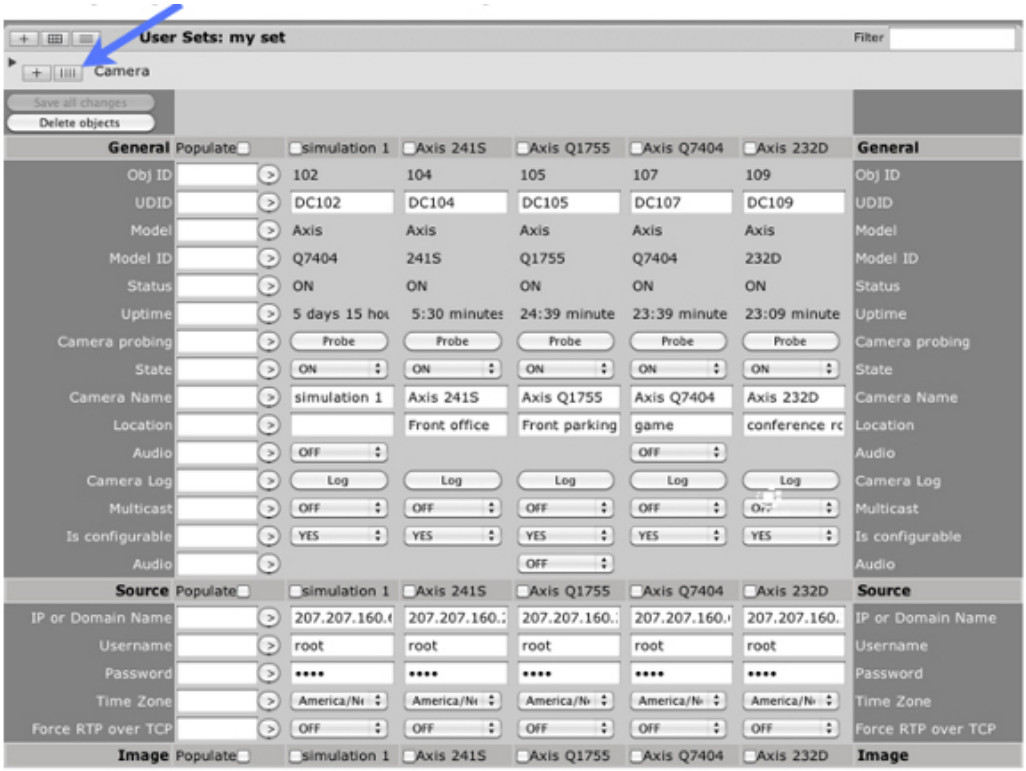


Figure 3.11. Mass Edit Cameras

Alternatively, when using the same screen, you can work on a camera-by-camera basis, but apply all the changes in one place by one operation.

The utility described will work with the cameras of one Set, so you have the flexibility to manage a group of cameras through their logical groups exposed in that Set. See *Section 4.4, "Users and Roles and Management"*.

3.5. Configuring Cameras

Please make sure your network camera is accessible over the network and you can identify basic information such as the camera model, authentication (username/password), etc...

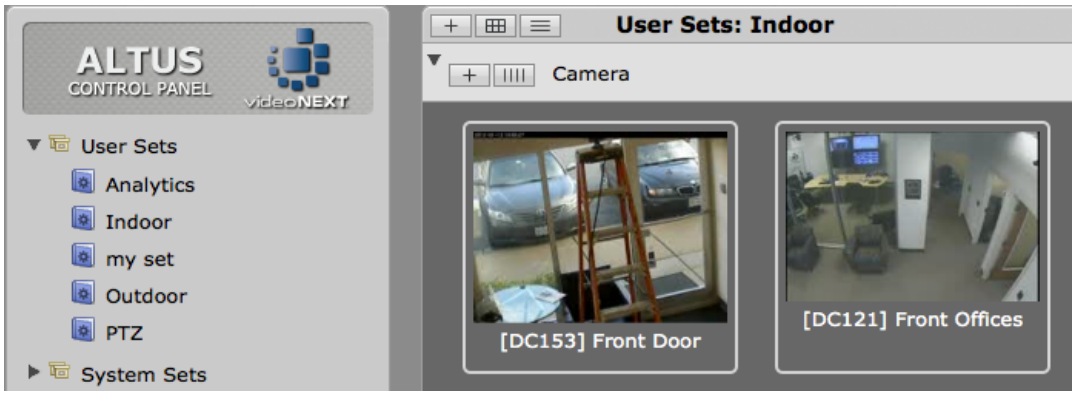


Figure 3.12. Camera Configuration

To add a new camera, click on the box with plus sign ("+") to the left of the "Camera" header. Options will appear. You will now be in the Add Camera Wizard.

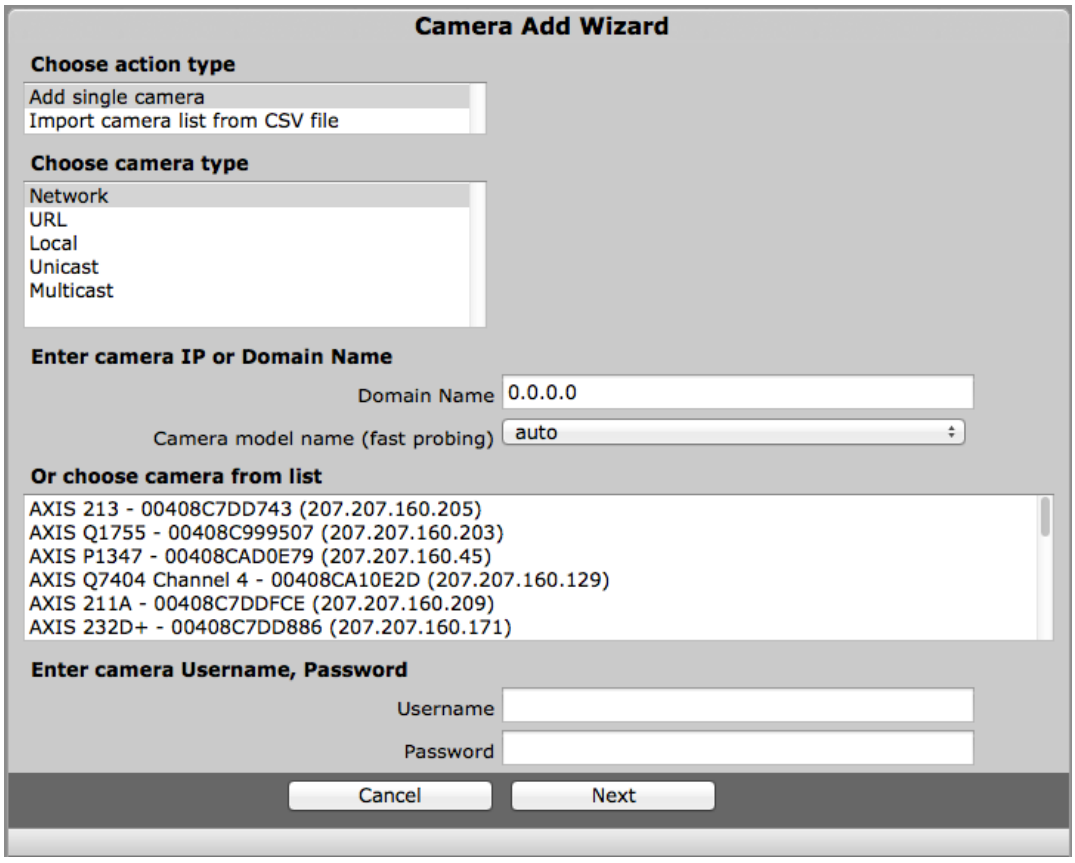


Figure 3.13. Camera Wizard

Here is a brief description of each option:

- Choose action type - You can choose either to add a single camera, or import multiple cameras from a CSV. The format of the CSV will be covered in *Section C.6, “Importing and Exporting CSV camera lists”*.
- Choose camera type:
  - Network - is for a networked camera that is supported officially by Stratus.
  - URL - Cameras that are not officially supported can be added here if you have the RTSP-URL for the video stream.
  - Local - This option is for cameras physically attached to the server, such as USB web-cameras.
  - Unicast - Unicast Port to listen on for an incoming MPEG2-TS connection.
  - Multicast - The Multicast address and port to subscribe to for MPEG2-TS multicast.
- Enter Camera IP or Domain Name - Here you can choose the IP address or Domain Name for the IP camera. (this assumes you have chosen to add a single network camera, this menu will change if you choose other options).
  - If you have an AXIS camera, you can optionally choose it from the list below. This list is generated automatically through a process called Zero-conf.
- Enter Camera Username, Password - You should enter the username and password required to access the camera. In most cases, you will want to use an account for the camera that has privileges to modify camera settings, but this is not required.

You can then click on the Next button.

The next screen will be a preview screen of the camera.

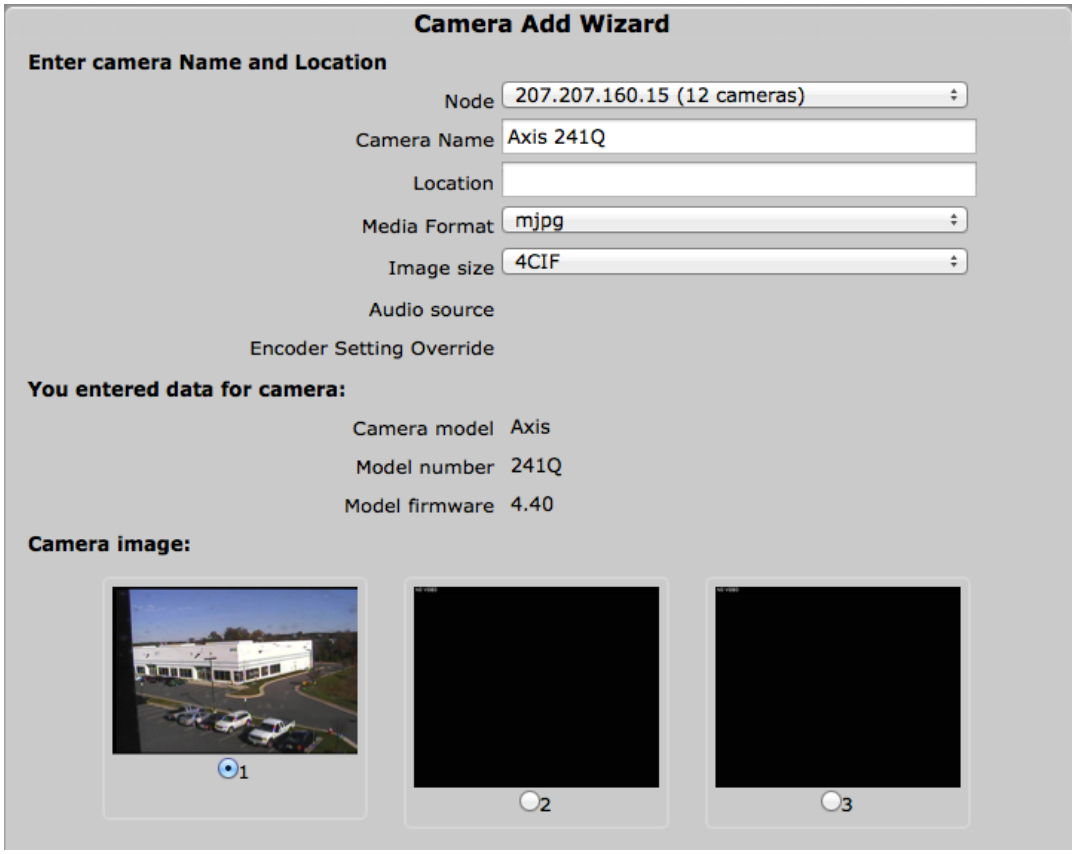


Figure 3.14. Preview

Here you can give a name and location, as well as choose the resolution and media format to use.

A snapshot of the camera will be displayed. If the camera that you added has multiple video feeds available (such as with a multi-port encoder) each video feed will have a snapshot, and you can choose which feed to use.

If you are using a multi-node system, you can also choose which node to place the camera on. The system will attempt to place the camera on the system with the fewest cameras, by round-robin.

Press Next.

Your system should now have minimal functionality. Please see *Chapter 4, Advanced System Configuration* for more configuration options.

Advanced System Configuration

4.1. Cameras

A camera's configuration page is broken in to multiple tabs. On each tab there will be a box displaying a snapshot from the camera, with a "Play" arrow to allow playing of video from that camera. The content of the tabs is dependant on the make and model of the camera, but the most common attributes will be listed below.

4.1.1. The General Tab

The General Tab displays the state of the camera on the system. It includes information like name, model, and status.

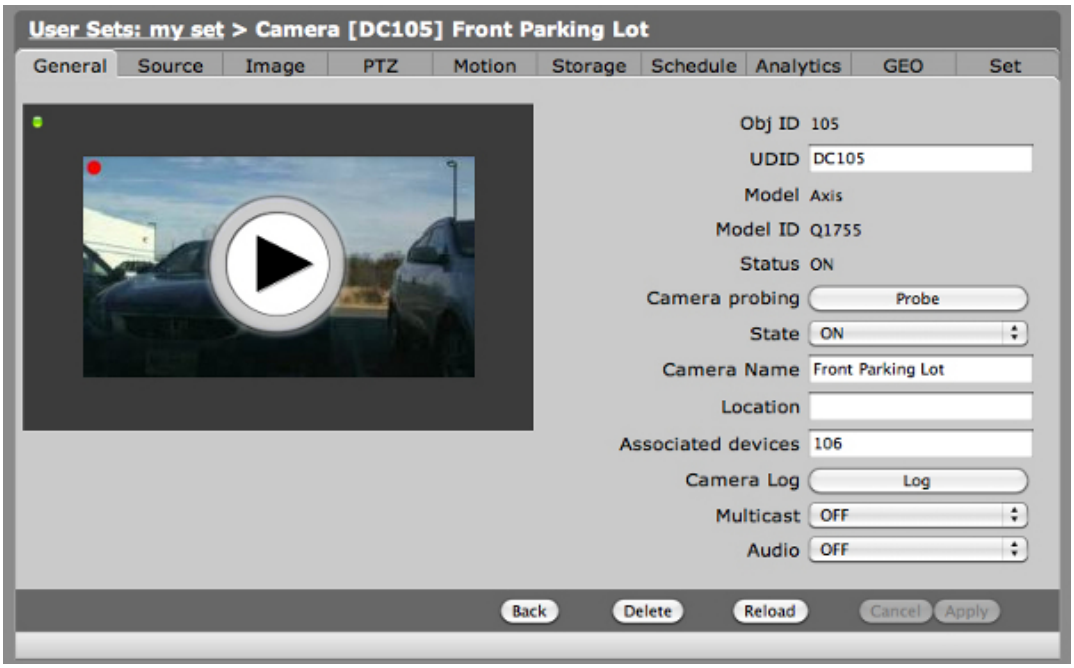


Figure 4.1. General Tab

Table 4.1. General Tab

Parameter	Description
Obj ID	This is the unique identifier the system uses to identify devices. Read Only.
UDID	This is the user-modifiable identifier. A default will be created automatically if none is provided.
Model/Model ID	This is the camera make/model, identified through automatic probing. Read Only.
Status	This is an indication of the current device processing state. It will go through “Starting” to “ON” and through “Stopping” to “OFF” upon setting the State to ON or OFF.

Parameter	Description
	The status will also display “Broken” or “Down” error codes. Use the “Refresh button at the bottom of the page to update as needed. Read Only.
Uptime	This lists the duration of the current network connection to the camera. If this duration is routinely very low, it may indicate a problem with the camera. Read Only.
Camera Probing	Pressing this button will force the camera to be re-probed, updating the camera make/model if it has changed.
State	This is set to “on” to allow this camera to actively operate. Set to “off” to disable.
Camera Name	This is how camera will be identified by Operators.
Location	This is a description of where the camera is located (e.g. “Building 4”).
Associated Devices	This is a list of the ID’s of associated device (such as audio-recording device)
Camera Log	Pressing this button will display a log of the camera's current activities. This button allows you to preview a realtime report of the internal system messages, where you might find reports on issues like wrong username/password, rejected connection, etc.
Multicast	This determines whether the video will be transmitted to users over multicast. The default setting is “Off”.

4.1.2. The Source Tab

The Source Tab controls how the system will attempt to connect to the camera.

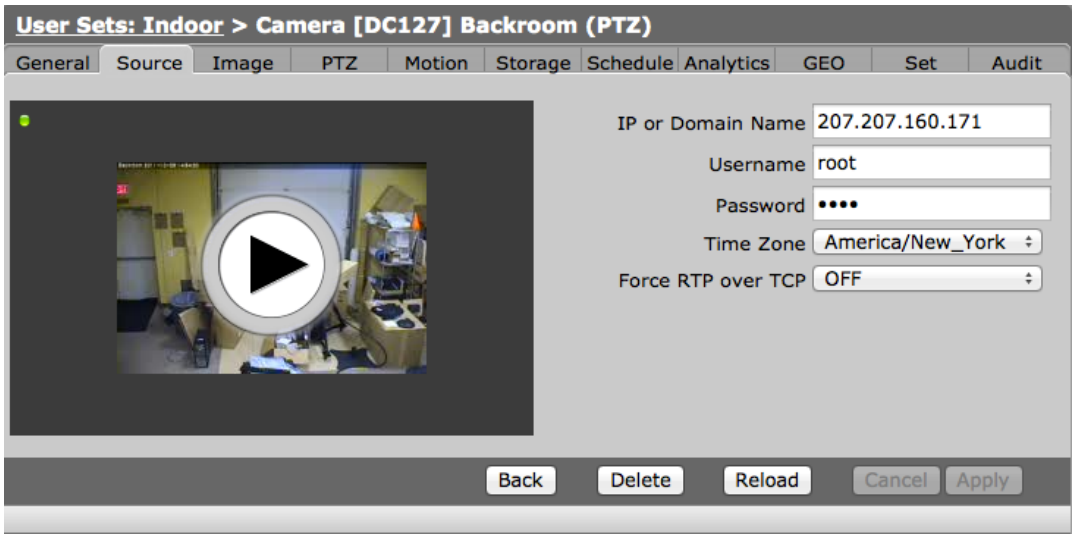


Figure 4.2. Source Tab

Table 4.2. Source Tab

Parameter	Description
IP address	This is the camera network address. Both IP and DNS name are supported
Username/Password	The correct authentication for accessing the camera. If not provided, the camera will not operate properly, or at all.
Input Number (optional)	The video input number for multi-port encoders. This will not be shown for devices which do not need it.
Time Zone	Stratus operates in Universal Time (UTC) and will allow you to support multiple cameras all around the world with a proper automated time calculus. Set the timezone the camera is in.
Force RTP over TCP (optional)	A choice to force the sending of video to the server over TCP. In some cases, setting to "On" will fix problems with receiving video. Default to “OFF”.

Note

Some cameras may show video, but disable the PTZ or other controls if you do not provide correct username/password

4.1.3. The Image Tab

The Image Tab controls what type of video should be retrieved from the camera.

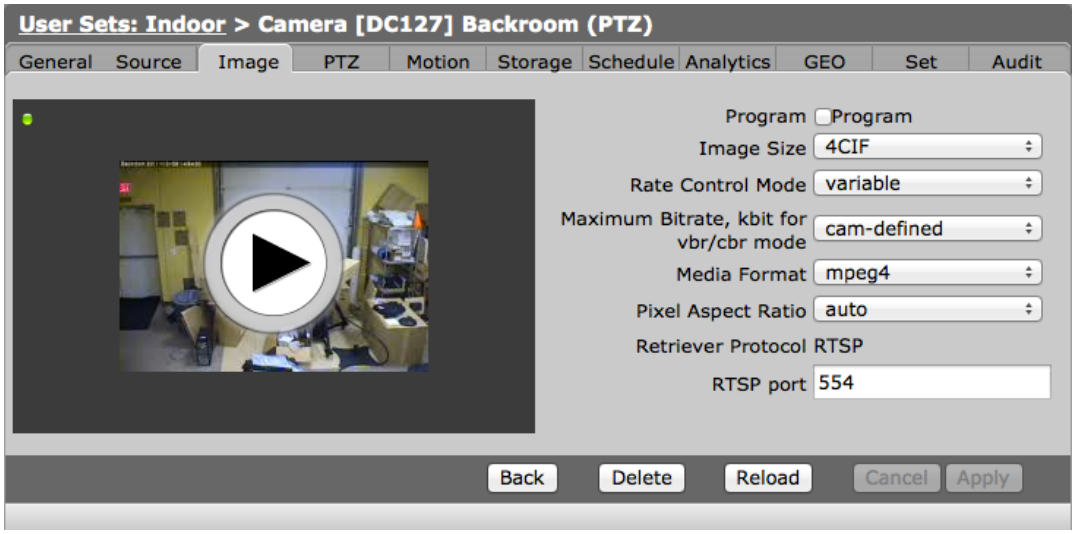


Figure 4.3. Image Tab

Table 4.3. Image Tab

Parameter	Description
Image size	For most regular cameras, the largest size will produce the best visual result at the cost of more bandwidth and storage utilization. Other options may be considered to reduce the load on your Storage and Network.
Frames Per Second (FPS) / *Bitrate*	These options directly influences video quality and the load on the Storage/Network. As a rule, the higher you set them the smoother video will be but the more resources it will take of the Storage and Network.
Media Format	This will be a list of supported video-stream formats. See *Appendix B, Video Codecs, Transmission Protocols and their Effective Usage* for a discussion on the pros and cons of each.
Retriever Protocol	This lists what protocol is being used to access the video, RTSP or HTTP.
RTSP Port / *HTTP Port*	If present, allows you to set which network port to use to retrieve video. Default for RTSP is port 554. Default for HTTP is port 80.

4.1.4. The PTZ tab

The PTZ Tab controls what driver to use to control any PTZ available to the camera.

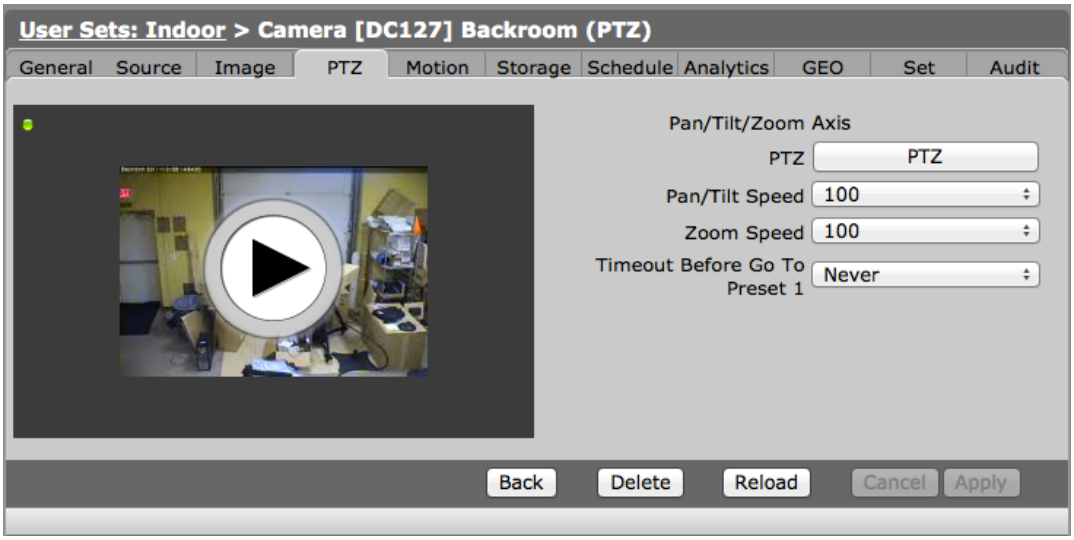


Figure 4.4. PTZ Tab

Table 4.4. PTZ Tab

Parameter	Description
Pan/Tilt/Zoom	This will list the current protocol the system will use for PTZ control. This option can be changed on encoders that support multiple PTZ protocols.
PTZ	This button will open a new window to allow control of that camera.
Pan/Tilt Speed	This allows movement speed to be scaled up and down.
Zoom Speed	This allows zoom speed to be scaled up and down.
Timeout Before Go To Preset 1	This is the number of seconds before the camera will automatically move back to Preset 1. Default is Never.

4.1.5. Camera Motion Detection

Stratus has multiple options for camera motion detection. They are all configured in the “Motion” tab of camera editor, “Motion Detection Engine” parameter.

Upon camera creation, the default value is “off” to limit unwanted event creation. Until calibrated, motion detection uses simple default settings that will not be tuned for the scene the camera is looking at.

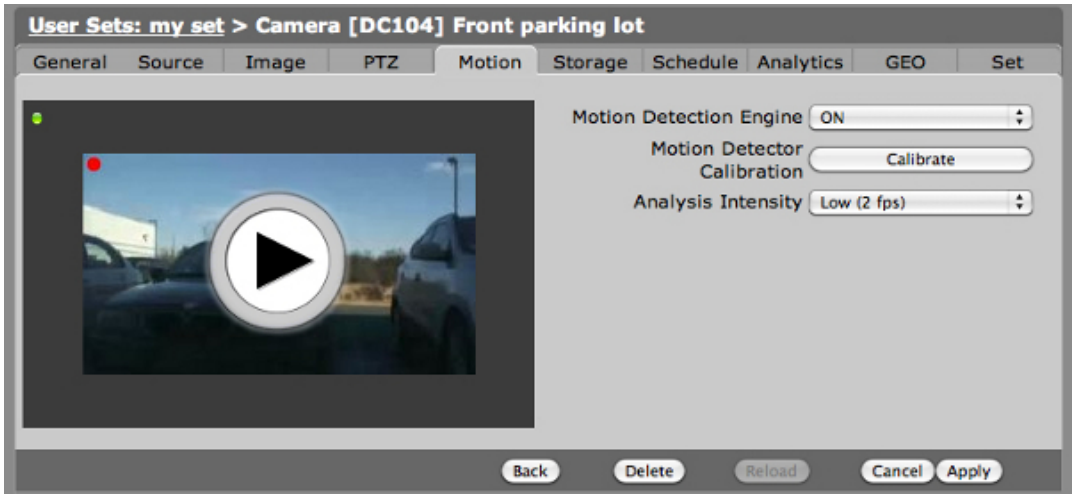


Figure 4.5. Motion Detection Tab

If you want the camera to utilize some sort of Motion Detection, you will have to use one of next values:

- "ON" - Stratus internal (software) Motion Detector will be used (advantages: any camera may use it, very flexible configuration options; drawback: additional load on server CPU, which is fairly moderate).
- “External” - camera internal (“external to Stratus”) motion detector will be used. This option works for Axis cameras only and allows the use of the camera's software motion detector.
- “Sensor” - camera wired connector for hardware motion detector (or other type of open/close sensor) will be used to detect motion events. This option is supported for IQeye cameras only.

In the majority of cases, the "ON" (or "Stratus software Motion Detector") setting is used, as this functionality is not very taxing on the system's resources, while providing a wide range of configurable options to accommodate a wide range of conditions normally found on security videos.

For Stratus internal software Motion Detector, a special “Calibrator” utility is provided, which is opened by clicking on the “Calibrate” button:

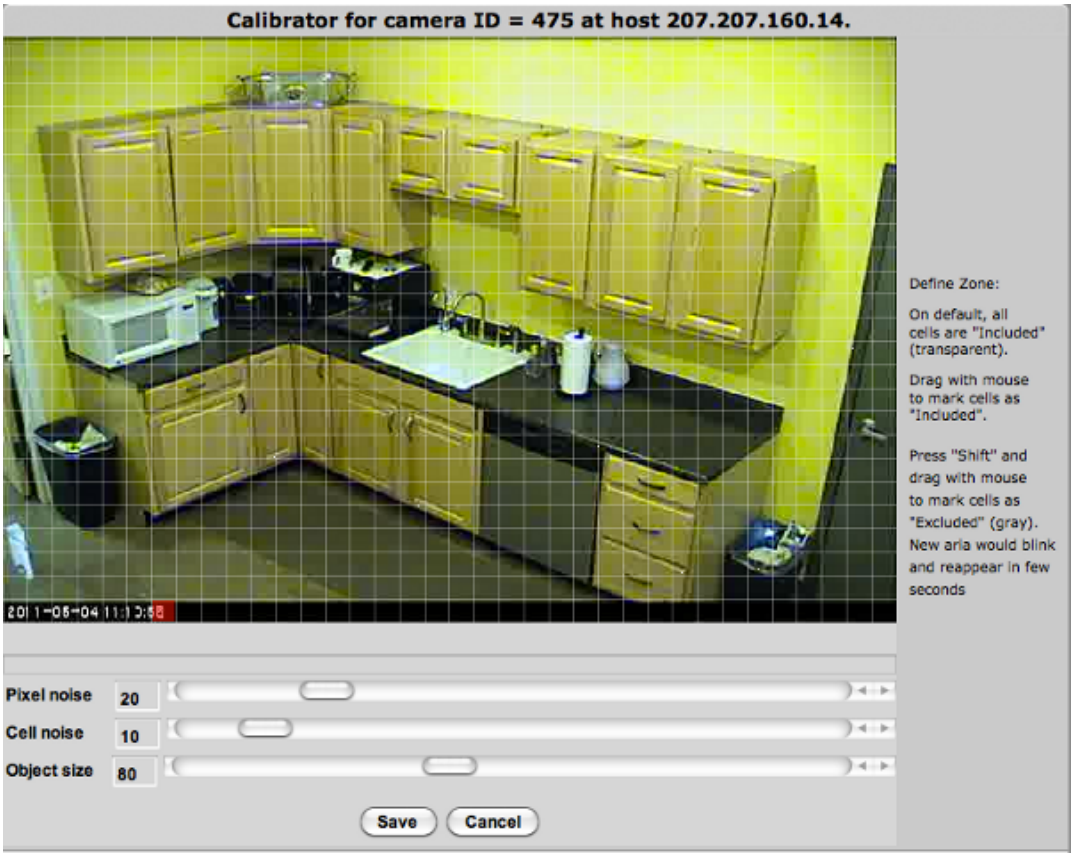

Calibrator for camera ID = 475 at host 207.207.160.14.
Define Zone:
On default, all cells are "Included" (transparent).
Drag with mouse to mark cells as "Included".
Press "Shift" and drag with mouse to mark cells as "Excluded" (gray).
New aria would blink and reappear in few seconds
Pixel noise
20
Cell noise
10
Object size
80
Save
Cancel

Figure 4.6. Motion Detection Calibration

Here, the real scene picture is presented to the Administrator, which is updated every second with a fresh image and additional information received directly from the Motion Detector. The algorithm is based on Background Subtraction and will detect changes in subsequent video frames with special provisions to ignore “normal” background changes.

The Calibrator screen shows partial detections as white dots on the top of the image, and you will notice that even perfectly still video will have these white dots around sharp edges or lines, which is attributed to the “Pixel Noise”. The Calibrator allows you to adjust the algorithm sensitivity to Pixel Noise based on a visual assessment in realtime, what simplifies camera calibration to particular scene and lighting conditions. Normally, some Pixel Noise should be present (to make sure you did not set threshold too high and ignore “real action”), but the amount of noise on the previous picture is slightly excessive.

The picture in the Calibrator is subdivided into Cells, which are analyzing the number of pixels with detections to determine if a Cell has motion or not. The second control in the Calibrator (“Cell Noise”) is utilized to adjust Detector Sensitivity to reliably detect motions and disregard Pixel Noise. To facilitate the visual calibration process, cells will be painted green/yellow/red dependent on the trigger threshold for the Cell Noise, where “red” depicts that “motion was detected in the cell condition, “yellow” is “very close”, and “green” is “some motion is present, but relatively low”. A Properly calibrated camera may show some “green” cells for non-moving areas, but should not have any “yellow” or “red”, while any small motion should reliably fire “red” detections.

Note

The “Cell Noise” parameter is very important for the “STD Motions and Events” Storage Policy as it determines the “Cell Trigger” point, which is used to decide if video should be recorded or discarded. Use “exclusion zones” to mask any areas of video where constant unwanted motion occurs (like waving trees in windows, water, etc..)

The “Object Size” parameter allows you to discriminate targets based on their size in Cells. In *Figure 4.6, “Motion Detection Calibration”*, “10” is sufficient to detect a person, even if only slightly in the frame, while disqualifying normal levels of "noise". When such a detection happen, a red border flashes around entire picture to visually alert about detection.

By default, the entire video area is INCLUDED, but the Administrator/Installer may elect to exclude any arbitrary number of Cells from the analysis to safeguard against unwanted detections (like waving trees in windows, water, etc..)

All the scenarios described above work as “what if?” controls. They do not introduce changes until you click on the “Save” button.

4.1.6. The Storage Tab

The Storage Tab will allow you to control how the video being stored on the system is handled.

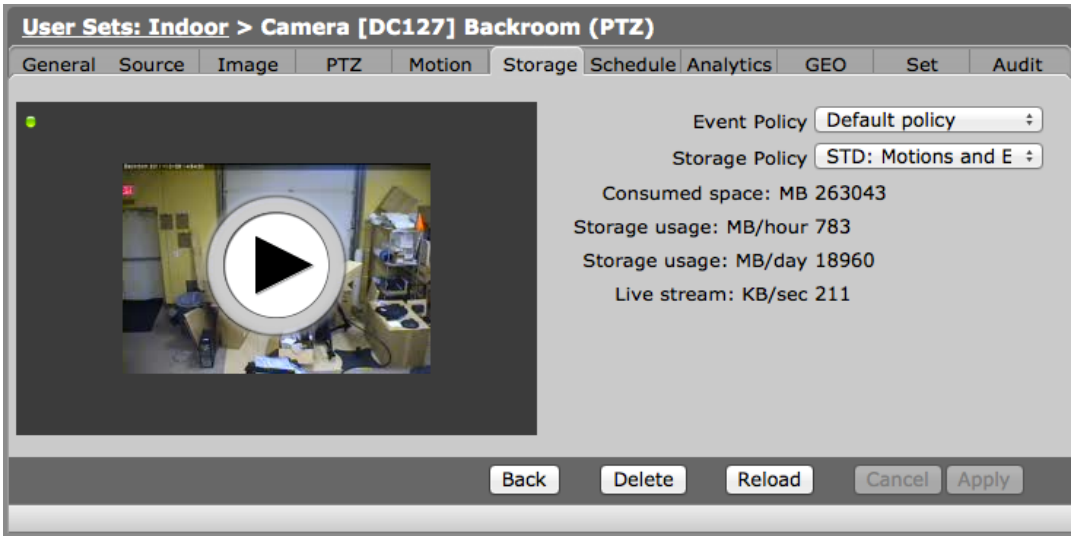


Figure 4.7. Storage Tab

Table 4.5. Storage Tab

Parameter	Description
Event Policy	Sets which event policy will be used for this camera. See *Section 4.6, "Configure Event Handling"* for more information.
Storage Policy	Sets which Storage Policy should be used for video storage. See *Section 3.4, "Manage Storage and Storage Consumers"* for more information.
Consumed Space	This is the total amount of storage that has been used by this camera so far in Megabytes.
Storage Usage	These two entries list the average amount of storage required per hour or per day in Megabytes.
Live Stream	This is the current bandwidth that is required to view/store live video from this camera in Kilobytes.

4.1.7. The Schedule Tab

The Schedule Tab allows you to set which schedule the camera should be subscribed to, if any.

Table 4.6. Schedule Tab

Parameter	Description
Schedule ID	A list of user-created schedules you wish to assign this camera to. Leave blank to not use a schedule For more information on how to configure Schedules, please see *Section 4.11, "Schedule Manager"*.

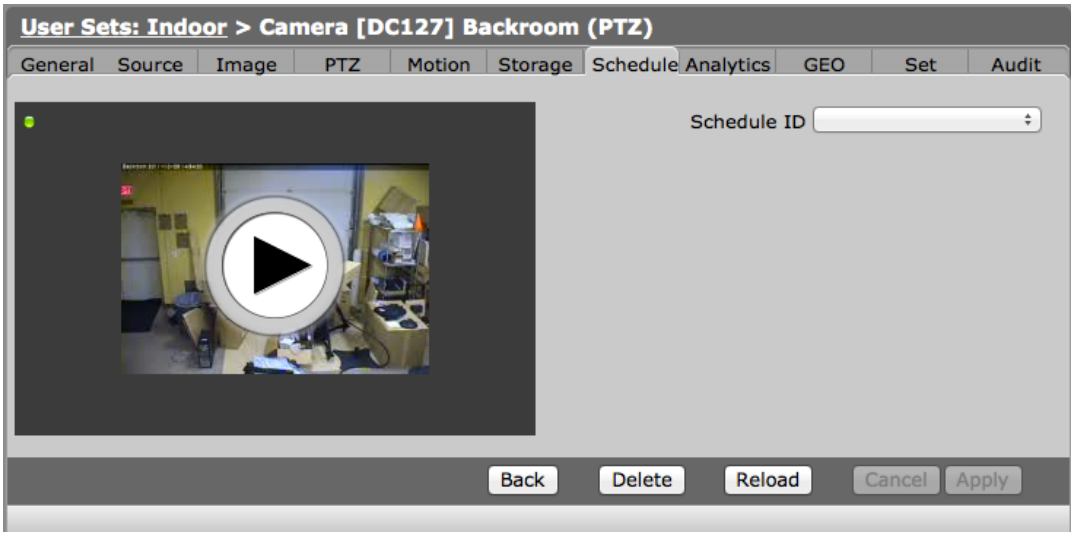


Figure 4.8. Schedule Tab

4.1.8. Analytics Configuration

"Analytics" is one of the options you may enable in Stratus to allow your digital video to automatically extract signaling information, which otherwise may require continuous human review and analysis.

In 3.3, Stratus supports three Analytics algorithms, ObjectVideo, VCA, and GMU. Other improvements include Trip Wire / Focus Region detections and target trail visualization for video-archive.

Note

Please note that the target-detection is triggered by the Object's bottom-midpoint (at the objects "feet") for both Trip Wire and Focus Region detection. This approach is more accurate in most situations.

The capability is similar to "Motion Detection" described in the section above, but can provide more granular feature extraction, such as Object Tracking and Behavior Analysis at the expense of more system resources (mostly CPU) utilized. Usually you can expect 5-7 times more CPU utilization by Analytics in comparison to Motion detection. This is largely dependent on video resolution and frame rate.

Analytics may be enabled on any fixed camera (PTZ-enabled cameras are currently not supported). Analytics are purchased separately, as this is not a part of the "standard" license in Stratus.

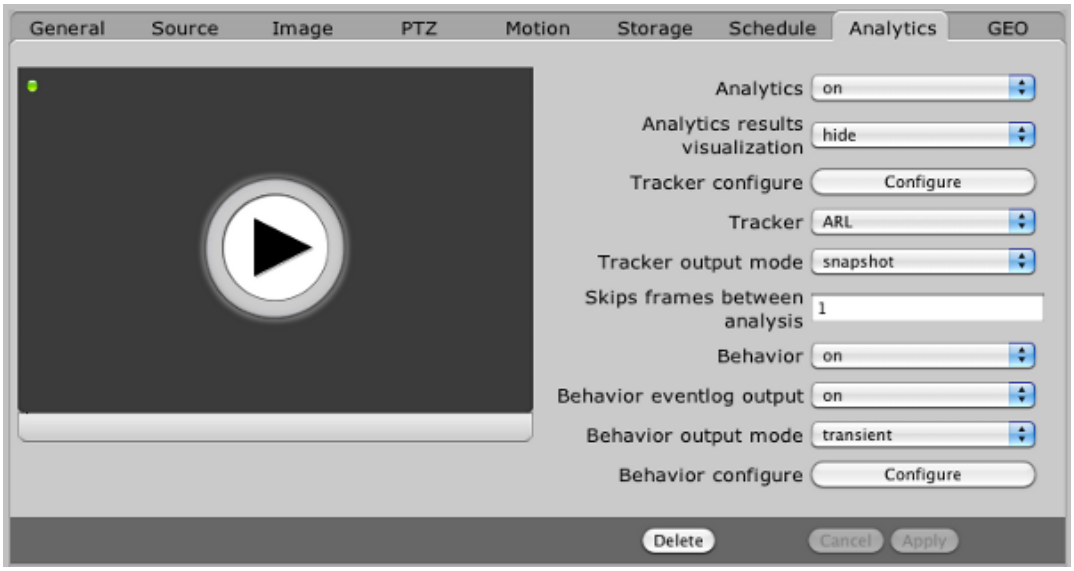


Figure 4.9. Analytics settings

To use Analytics, you need to enable it first by changing the “Analytics” setting to “on” in the “Analytics” section of the Camera Configuration Utility of Admin Interface.

Table 4.7. Analytics parameters

Parameter	Description
Analytics	Turn *ON/OFF* the Analytics Engine
Tracker	Which tracker to use: OFF - no tracker. SSVA/OV - Server-Side Video Analytics, Object Video. SSVA/VCA - Server-Side Video Analytics, VCA. SSVA OV+VCA - Server-Side Video Analytics, using both Object Video and VCA algorithms at once.
Analytics Results Visualization	Four Options are available: *Disable*, *Alerts Only*, *Tracks/Alerts*, and *Tracks/Alerts/Rules*. *Disable*: Analytics Results are generated, but not visualized over the video. *Alerts Only*: Analytics Results are generated, but visualized on-demand only (“analytics” icon allows Operator to enable visualization). *Tracks/Alerts*: Analytics Results are generated and displayed on the Operator Interface as green bounding boxes. *Tracks/Alerts/Rules*: Like *Tracks/Alerts*, but it will also show which configured rule was violated
Tracker Configure	This option will open a new window to fine tune tracker settings; details provided later

Parameter	Description
Skips Frames between analyses	Number of frames skipped for every frame analyzed. This number depends on 1) Frames per Second (FPS) and 2) the complexity of the scene (speed and size of the object, distance, lighting conditions etc.) As a "rule-of-thumb", ensure that the object is analyzed at least 7 to 12 times per second. For 30 FPS, choosing 3 will ensure that 7.5 frames are analyzed per second.

Once these basic settings are properly configured you will have to Apply the changes. From this point you can start configuring the Tracker and Behavior Analyzer. More information can be found in *Appendix A, Analytics*

4.1.9. Camera GEO-Calibration

The Stratus Operator Interface allows the use of Google Earth© within the browser to visualize cameras and Events, and work with Live Video and PTZ operations. This functionality will be enabled automatically once the Administrator GEO-calibrates one or more of the cameras.

To calibrate a camera you have to open the camera settings editor and go to the “GEO” tab:

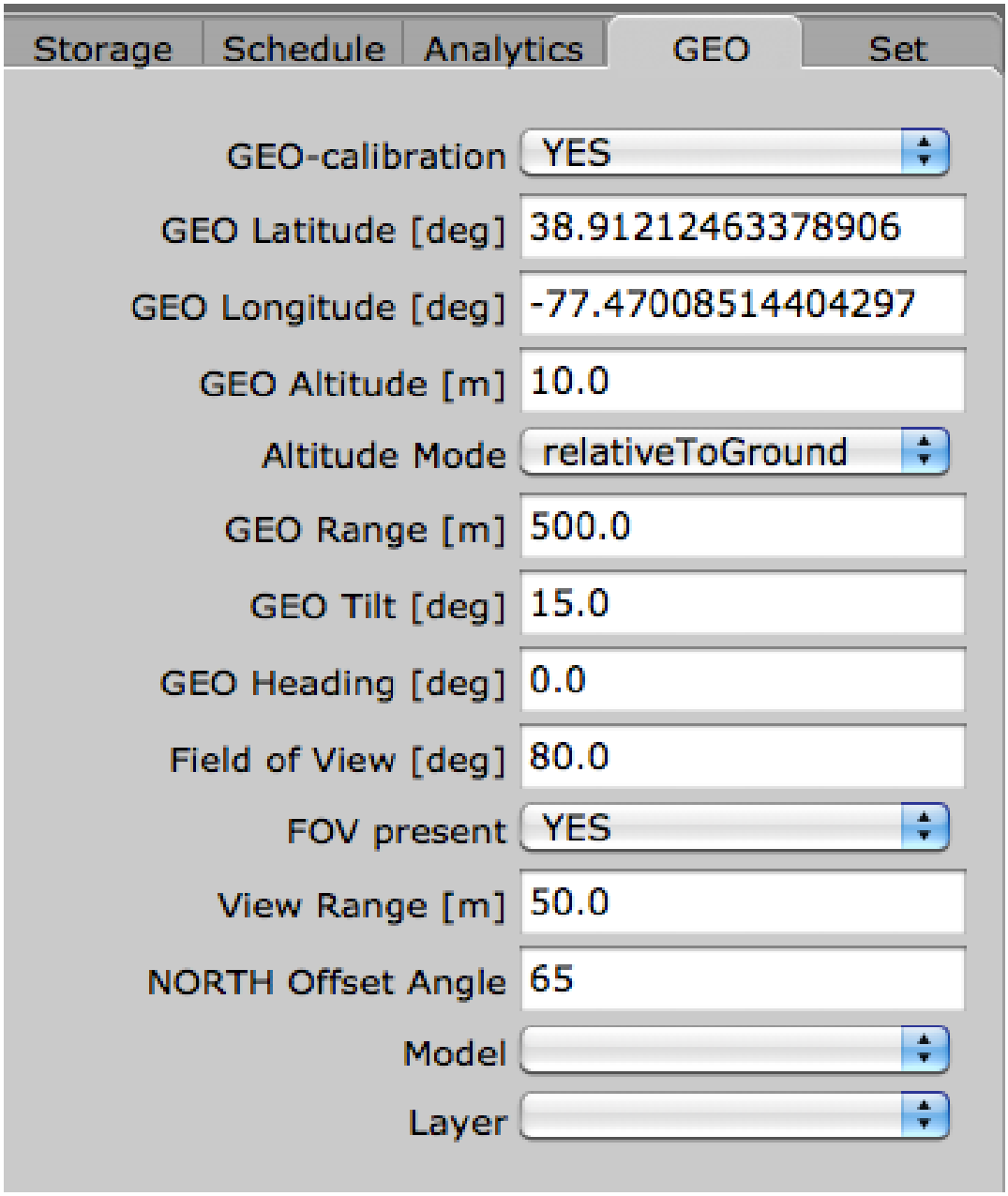


Figure 4.10. Geo Editor

The options on this tab are:

Table 4.8. The GEO Tab

Parameter	Description
GEO-calibration	[YES/NO] - The following options will only be displayed if set to "YES".
GEO Latitude	The Latitude of the camera, in degrees and fractional degrees (not minutes/seconds). It is recommended to be as precise as possible.
GEO Longitude	The Longitude of the camera, in degrees and fractional degrees (not minutes/seconds). It is recommended to be as precise as possible.
GEO Altitude	The Altitude of the camera, in meters. It is recommended to be as precise as possible.

Parameter	Description
Altitude Mode	[RelativeToModel/RelativeToGround/Absolute] - This sets whether the listed GEO Altitude is relative to the loaded model, the ground level, or above sea level.
GEO Range	The range above the camera of the default Google Earth view, in meters.
GEO Tilt	The tilt of the default Google Earth view, in degrees.
GEO Heading	The default Orientation of the Google Earth view, in degrees.
Field of View	The horizontal Field of View for the camera, in degrees.
FOV Present	[YES/NO] - Sets whether to show the FOV cone on the Google Earth map, or not.
View Range	Distance the camera can see, in meters. This sets how long the FOV cone will be.
NORTH Offset Angle	The degree offset from True North the camera is looking. This is can be calibrated easily for PTZ cameras using steps detailed below.
Model	Sets the camera to appear on a specific Model. (Optional)
Layer	Sets which layer of the model to display the camera on. (Optional)

If the camera has already been calibrated you will see the map centered on the current camera position. Otherwise, you will have to switch the “GEO-calibration” parameter to “yes”, and select a camera position while navigating through the Google Earth's three-dimensional map. To place (or relocate) the camera, click on the camera icon in the legend and then click on the map in the location where the camera is to be placed. Click “Save” to accept the change.

The GEO-calibration procedure has a second (optional) part relevant to PTZ cameras, which allows users to calibrate the camera's pan and tilt offsets for “slew” operation when receiving targets from a radar (or other type of device) providing GEO-coordinates for the targets. This functionality is available for integration through API and needs to be mapped to a particular targeting device like radar

To perform PTZ calibration, click the target icon in the legend, theno place the target over some distinct marker in the surrounding area (such as a pole, building corner, etc..). Open the video either by clicking on the camera icon or on the “play” icon in the video snapshot in camera settings section. It will attempt to center the camera over your marker object, but most likely it will be significantly off the marker since the settings are not yet correct. Now you have to use the ruler and up/down arrows (displayed above the map) to visually center the camera on your marker's projection to the ground. The ruler allows you to pan the camera left or right on every click of the mouse the number of degrees shown at the position of the click.

Once you are satisfied with camera alignment over the marker, move the target to another marker and confirm calibration accuracy. You might need to do minor adjustments to get reasonable accuracy. Click “Save” to accept changes.

The Administrator may also upload KMZ/KML models for multiple buildings and/or floors into Map3D and place cameras and Access Control objects into these models. Go to Settings->Customize system->3D Maps in left menu to open relevant management screen:

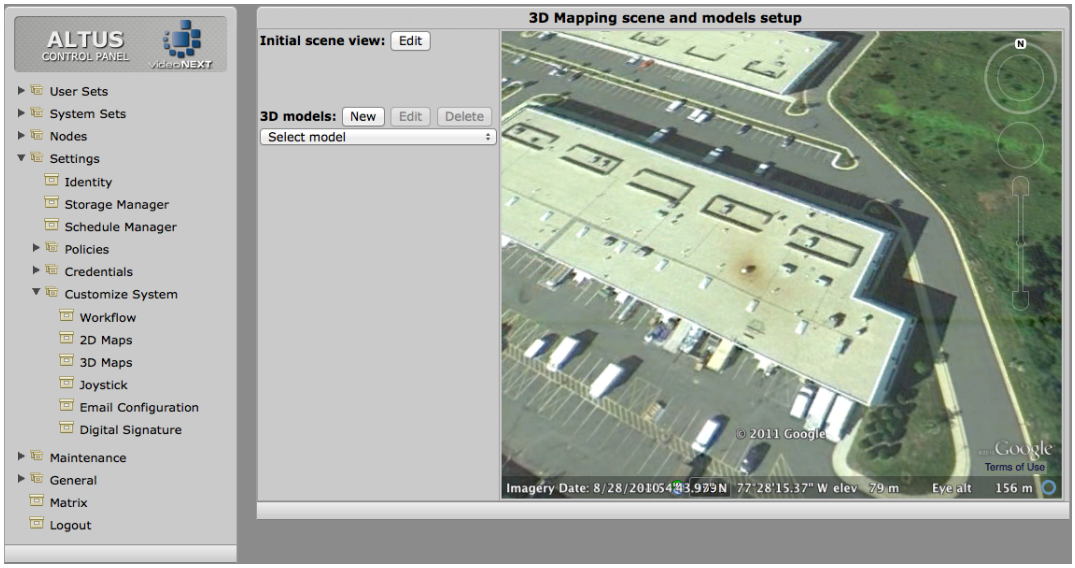


Figure 4.11. 3D map additions

3D models are created using the popular Google SketchUp Pro software, which allows you to define your own 3-dimensional model[s] or to import AutoCAD drawings. To create multi-layer (multi-floor) scenes, you need to export the model in a series of floors and upload them individually.

The device editor (see above) in the Control Panel allows the Administrator to associate camera/sensor/etc.. to models uploaded and managed with “3D mapping scene and models setup”.

The Operator is able to visualize these model[s] and associated cameras and objects, while slicing building[s] for convenient scene visualization.

4.1.10. The Set Tab

The Set tab allows you to assign the camera to any number of user sets (or none). Check the box next to any set you want the camera to be in. You can find more information about Set management in *Section 4.4, “Users and Roles and Management”*

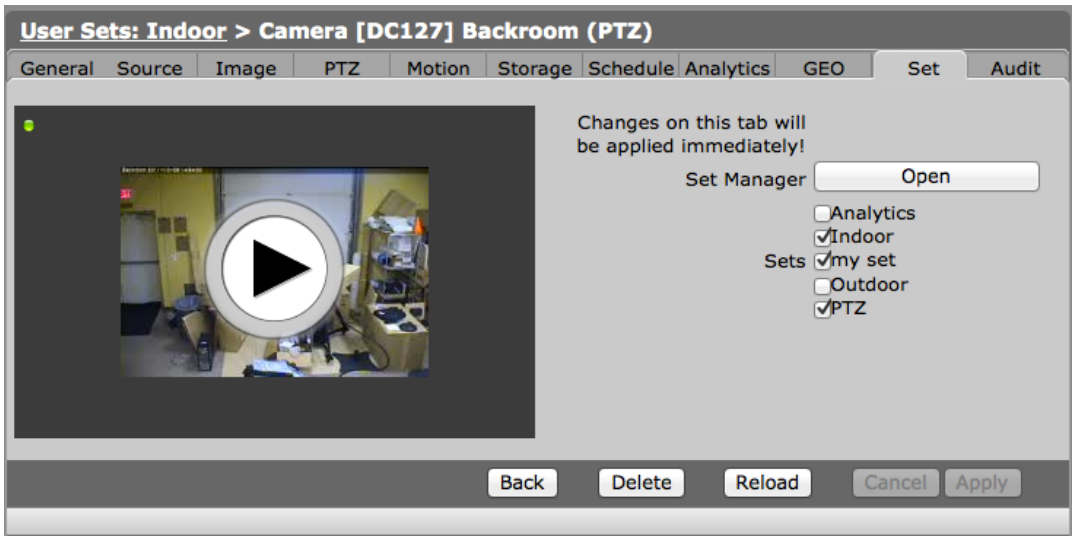


Figure 4.12. Set Tab

4.1.11. The Audit Tab

The Audit tab lists the activity with regards to this particular camera. For more information about the Audit log, see *Section 4.3, "The Audit Log"*.

The option "Show User activity" will show when a user requested live video, archive video (and what time period of archive), or controlled the cameras PTZ. Most entries can be expanded to give more information. For example, if you expand any User entry, you will see what IP address the user connected from. As another example, if you expand a "camera health" update, you will see what state the camera was in before.

The log is broken in to multiple pages. The first page will show the newest entries. If you need to view older entries than are shown on your page, you can enter an arbitrary page, or click "Next" or "Prev" until you find the correct page.

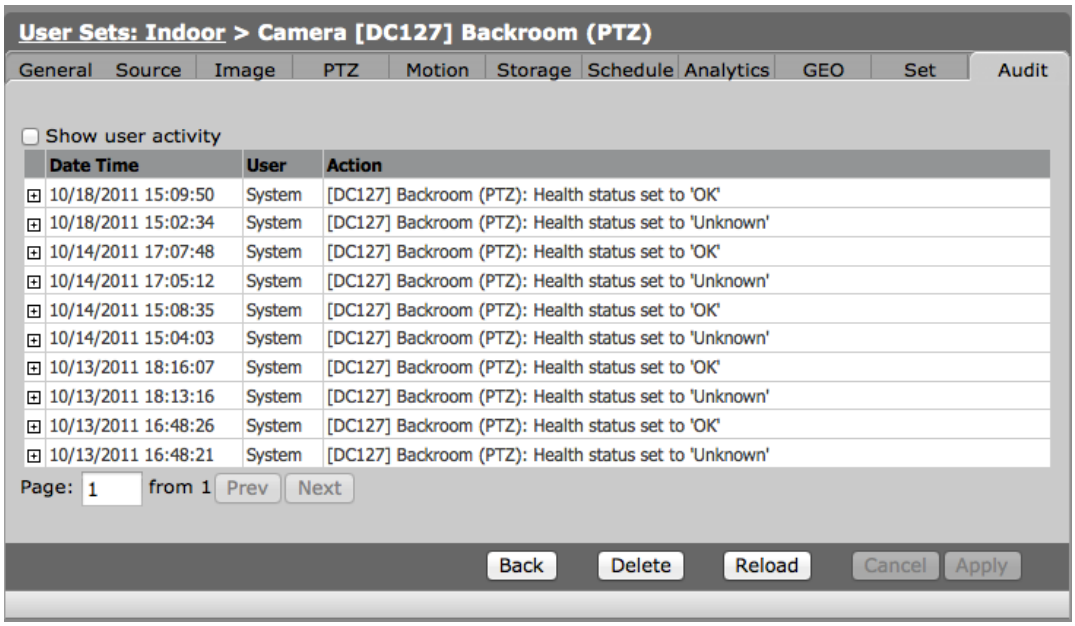

User Sets: Indoor > Camera [DC127] Backroom (PTZ)
General
Source
Image
PTZ
Motion
Storage
Schedule
Analytics
GEO
Set
Audit
Show user activity
Date Time
User
Action
10/18/2011 15:09:50 System [DC127] Backroom (PTZ): Health status set to 'OK'
10/18/2011 15:02:34 System [DC127] Backroom (PTZ): Health status set to 'Unknown'
10/14/2011 17:07:48 System [DC127] Backroom (PTZ): Health status set to 'OK'
10/14/2011 17:05:12 System [DC127] Backroom (PTZ): Health status set to 'Unknown'
10/14/2011 15:08:35 System [DC127] Backroom (PTZ): Health status set to 'OK'
10/14/2011 15:04:03 System [DC127] Backroom (PTZ): Health status set to 'Unknown'
10/13/2011 18:16:07 System [DC127] Backroom (PTZ): Health status set to 'OK'
10/13/2011 18:13:16 System [DC127] Backroom (PTZ): Health status set to 'Unknown'
10/13/2011 16:48:26 System [DC127] Backroom (PTZ): Health status set to 'OK'
10/13/2011 16:48:21 System [DC127] Backroom (PTZ): Health status set to 'Unknown'
Page: 1 from 1 Prev Next
Back
Delete
Reload
Cancel
Apply

Figure 4.13. Audit Tab

4.1.12. Email on Events

The system can be configured to send notification emails when events are generated. Each user can have an associated email address where event notifications will be sent to, and each device set can be configured to send events or not, to all users of a particular role.

To configure a user to receive email alerts on events:

1. Log in to the web interface as an admin user, and enter the Control Panel.
2. Chose Settings->Credentials->User Manager and set an email address for the user. You can also set an email interval to defines how often user will receive emails.

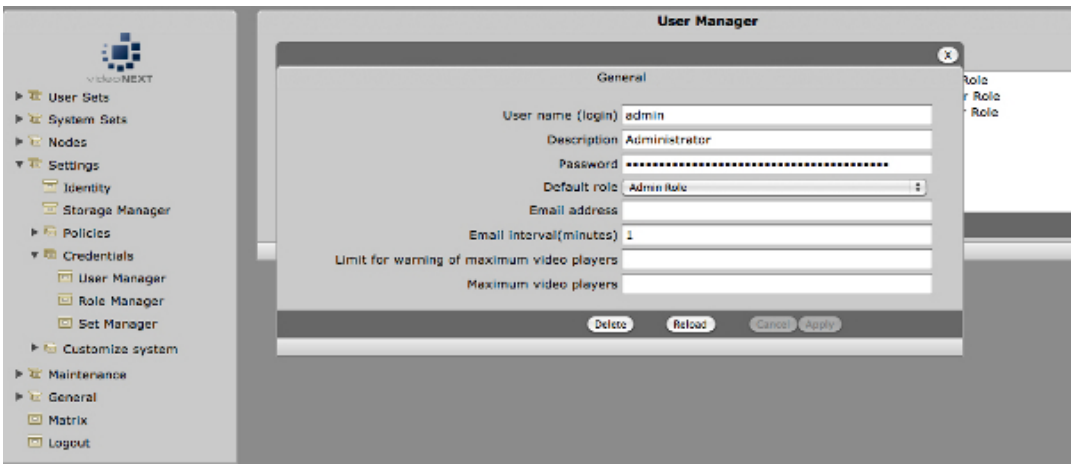


Figure 4.14. User Email

3. Under Credentials->Role Manager, find a role that is assigned to the user that is to receive emails. For each device set for which you want emails generated, click the "Email on Event" check-box. All devices in this set will send emails on alerts to all users in this role.

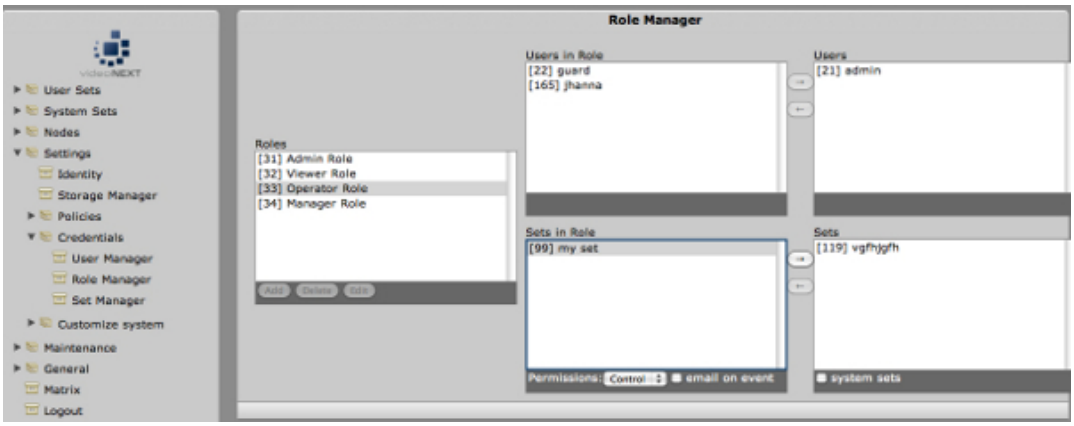


Figure 4.15. Role Email on Event

Setup the SMTP server

The Stratus system cannot send emails directly. Instead it sends emails using an existing email account. This email must allow SMTP POP3 access.

1. Go to Settings->Customize system->Email Configuration.

Figure 4.16. Email Configuration

2. Provide the SMTP server (such as smtp.gmx.com).
3. Provide credentials for the email account the Stratus server should send emails from.
4. Change the "Run Status" to YES.
5. (Optional) Create a test event to verify that the setup is working correctly.

4.2. Configuring DNS, NAT and Firewall

The very first step to make your Stratus system operational in a NAT/Firewall environment is to configure your Stratus server[s] to properly work with the DNS. If you do so, your nodes' names will appear by their real host names in the Control Panel's "Nodes" list.

Host names will be preserved from the client side when addressing servers, while the domain suffix can change when addressing the server from inside or outside the NAT/Firewall. For example, the host(s) may be addressed from inside as "alpha.local.lan" / "beta.local.lan", while they may be visible as "alpha.corp.company.net" / "beta.corp.company.net" from the outside. Both external names may be resolved to the very same external IP address, but both names should be resolvable by the DNS to the individual servers or video streaming from other non-master nodes will not work.

A firewall should be configured to have port 80 (HTTP) and 10000 (Stratus messaging) to accept incoming connections from outside NAT/Firewall. Both of these connections are over TCP.

In addition, each node's Real Time Streaming Protocol (RTSP) port (which can be found in the "Node Info" screen of a particular node) should accept connections from the outside, using UDP. In multi-node configurations, Stratus allocates the RTSP ports for its nodes with a five-port "pitch" starting from port 8554 (e.g. 8554, 8559, etc.). The pitch makes it possible to use one external IP address for multiple nodes, which are accessible through the RTSP from outside the NAT/Firewall. This is specifically done to avoid using Port Address Translation (PAT), which is problematic in some routers.

4.3. The Audit Log

The Audit Log is a new feature in 3.3. It records what happens with each device on the system, who changed settings, who accessed video streams, who controlled the PTZ, how the health of each camera has changed, etc.

The Audit Log can be accessed from two places: you can access each cameras audit log in the configuration settings of that camera, or you can view all devices in Maintenance->Audit Log.

If viewed from the Audit Log page, there are many ways that you can filter the Audit Log:

- You can filter based on the time interval, setting the Start and End time to search for.
- You can filter based on the Category of the log.

You can set the Start and End Intervals to filter based on time.

4.4. Users and Roles and Management

The Stratus Credentials Management system consists of four layers:

- Resources (cameras, sensors, etc..)
- Sets (resources grouped together)
- Roles (coordinated collections of Sets and Permissions)
- and Users

Resources are assigned to sets, and sets are assigned to Roles (with privileges), and Users are also assigned to Roles. A single resource may exist in multiple sets, and a single Set may be assigned to multiple Roles (and possibly with different permissions per Role). A Role can have multiple Users assigned to it, and a User may also belong to multiple Roles.

To avoid overcomplicated configurations as the system grows, Stratus does not allow individual Resources to be assigned directly to Users. Resources will always have to be assigned through Roles and Sets, even if a “flat” configuration is required.

Note

Stratus predefines and automatically maintains a "My Set" Set and "Admin"/"Guard"/"Manager"/"Viewer" Roles for convenient management of simplified (“flat”) configurations.

4.4.1. User Access and Permissions

The illustration below provides a “big view” on how credentials are managed in Stratus:

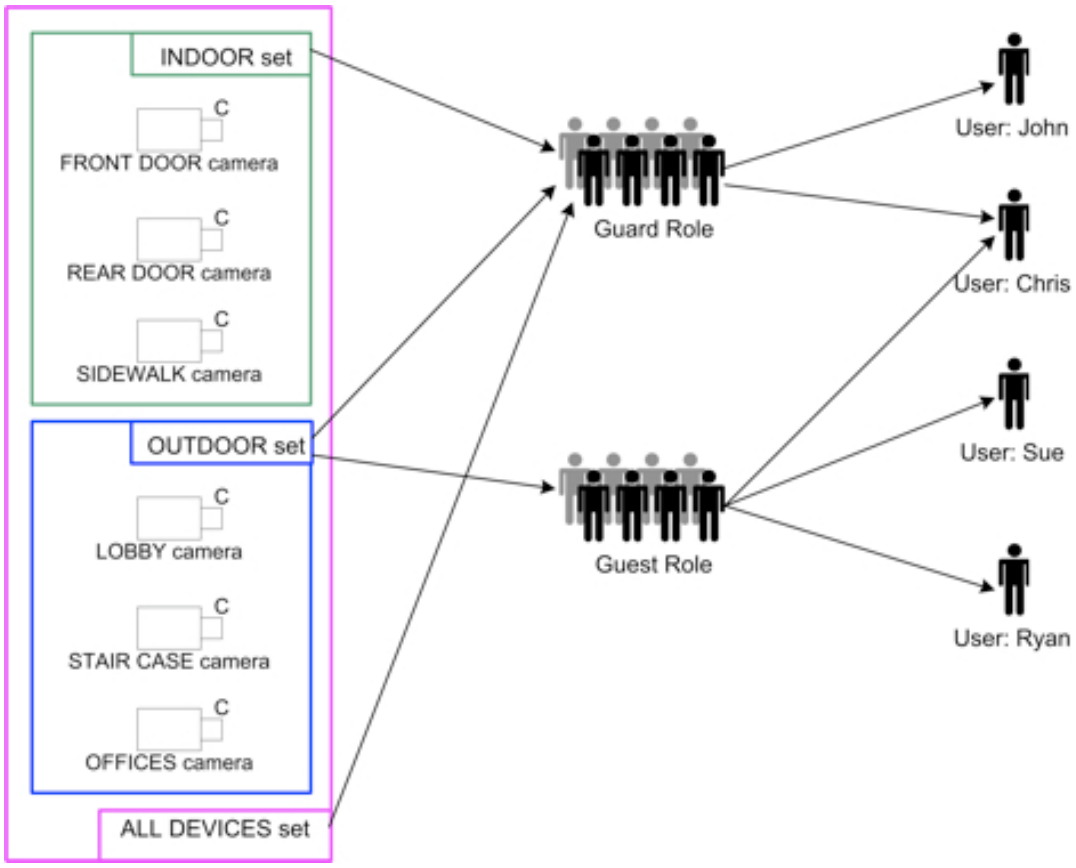


Figure 4.17. Credential management overview

Here (in simplified form) you see the most important concepts behind the Credentials Manager: Resources, Sets, Roles and Users.

Resources are the actual Devices with which Users will interact: Cameras, Sensors, Control Devices, Video Walls, etc.

The same approach is used when using the Operator Matrix or the Control Panel user interfaces. The Operator Matrix is automatically associated to any Admin-created Role, while the Control Panel is granted only through system-managed Admin Role. This also provides access to the system-maintained standard “All Cameras” / “All Sensors” / etc... Sets, which cannot be edited.

Sets provide an aggregation method for presenting the Resources in uniform pools managed together in the Operator Matrix User Interface. Resources are aggregated into Sets and then proper Permissions are granted for entire set on the [next] Role level.

One Role may combine one or more Sets, and similarly one Set may be used in multiple Roles. This provides a flexible mechanism of reusing aggregations when creating combinations of Resource Sets and Permissions for a particular Role. Since it is possible that one device may be published via two different Sets, which may be presented to the Role with different Permission levels, the final Operator Matrix User Interface will consolidate and use a superset of granted Permissions for consistent user experience.

Users provide an entity to map a real-world person into virtual object in the software, which has one or more Roles granted to perform manipulation with Stratus objects in one or more User Interfaces. If a

User is granted more then one Role - he/she will have to select or choose their Active Role, but only one role can be active at any given moment in time. This is needed to guarantee uniformity among multiple users who share the same Role, and it accommodates for real-life scenarios like a “temporary substitute” or “working in time-shifts”.

4.4.2. Resources and Sets Management

To manage Resources (and Sets at the same time) please open the “Credentials” menu on the left side, and open the “Credentials”/“Set Manager” screen. The next screen will open:

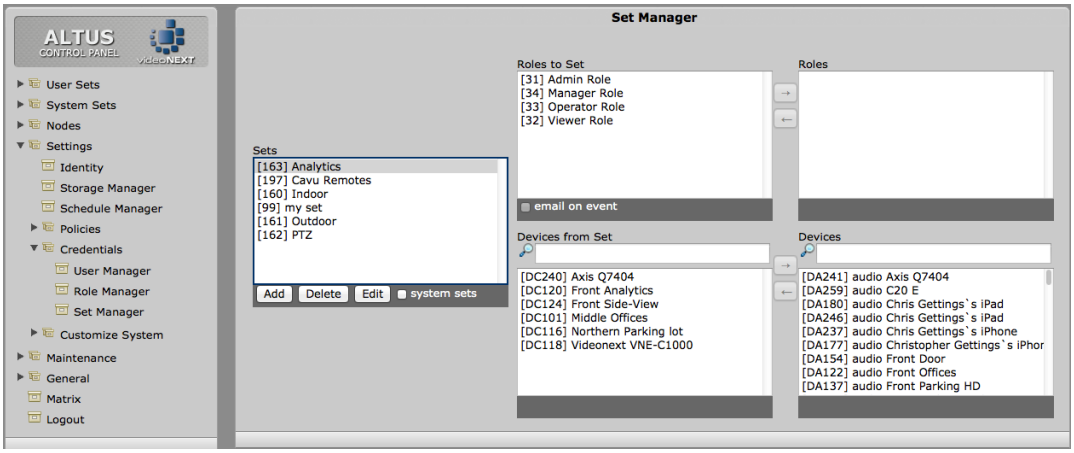


Figure 4.18. Set Manager

Here, the focal point is the “Sets” list. Upon selection you will see the associated Roles and those that can be assigned to that set.

The two boxes on the far right hand side of the screen are all roles and all devices not currently associated with this set. The two boxes in the center are for the roles and devices already associated with this set. Highlighting any Role or Device will allow you to assign/un-assign it from the currently selected set.

To create a new Set, click the "Add" button in the left-most box. This will open a dialog to name the set and provide an optional description. Once added, you will need to assign Roles that can view the set and devices belong to the set.

To delete a Set, select it and press the "Delete" button. You can only delete "User Sets", you can not delete System Sets (such as "All Cameras"). Deleting a Set does not alter the devices in that set.

When selecting a Role in the "Role to Set" box (top-middle), you will be given the option to enable "email on event" (this is only available for user-generated Roles).

4.4.3. Role Management

The Roles management screen is very similar to the Sets management screen explained above.

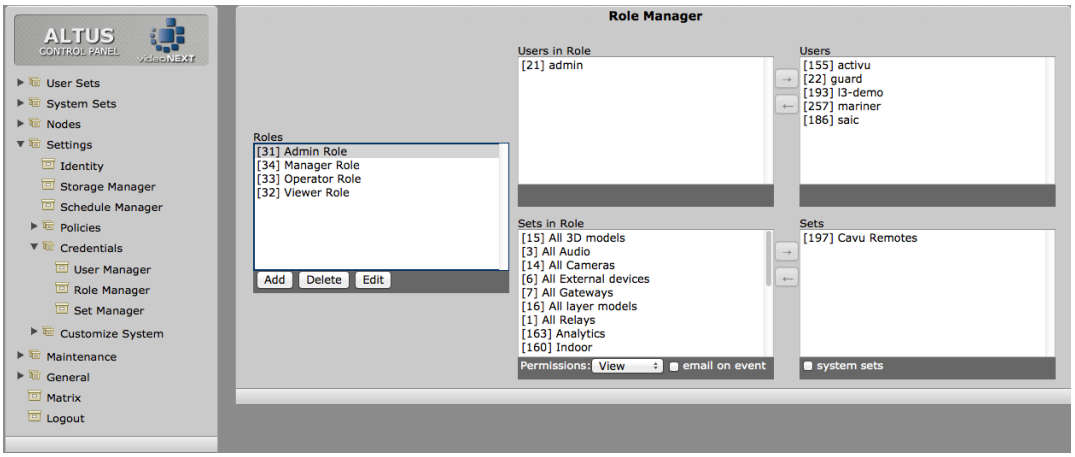


Figure 4.19. Role Manager

Here you can manage Roles, while associating Sets to Roles and Credentials assignment between Sets and Roles.

Much like for Set management, to add or remove a Set or User to a Role, highlight the Set and click the left/right arrow button. When a set is assigned to the Role, you can also choose the Permission level.

There are three permissions that can be assigned. Each subsequent permission includes the lower permissions. The lowest permission level is “View”, which only allows the user the ability to view live video from a camera. The next level is “Control”, which adds the ability for the user to control the camera through PTZ and to view archive video. The highest permission level is “Manage”.

The "Admin Role" is a special system-created Role. Only users assigned to this Role will have access to the administrative GUI. No user-created Role can gain this privilege.

If PTZ Prioritization is enabled in Settings->Identity->Miscellaneous, there will be an option in Role->Edit to set user PTZ-Priority level. The lower the number, the higher the priority. More information can be found in *Section 4.1, “Cameras”*.

4.4.4. User Management

The next screen allows for easy Users Management:

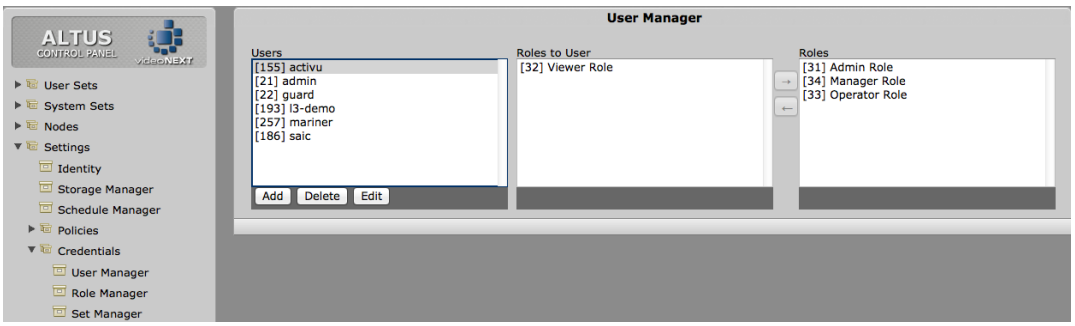


Figure 4.20. User Manager

User Management in Stratus is simplified by assigning a User to one or more Roles. It allows for easy Credentials reallocation for the pool of users.

Note

A User can only use one Role at a time. If multiple Roles are accessible for particular Users, then the user will be allowed to select a current Active Role, but only be able to use one Role at any given time. This is not a software limitation, but a mechanism to keep the user experience consistent among multiple Users working in concurrent environments.

When adding or editing a user, you will be given the option to set the name, description, and password. You can also input an email account, if you want events from certain devices to be sent to this user via email.

4.5. Storage Policies Management

Stratus software comes pre-configured with a set of default storage policies, which will perform well with any size storage system. This section is mainly concerned with additional features, not the mandatory configuration steps.

Please open the “Settings->Policies” section in the left menu of the Admin Interface and select “Storage Policy” to load the Storage Policy list.

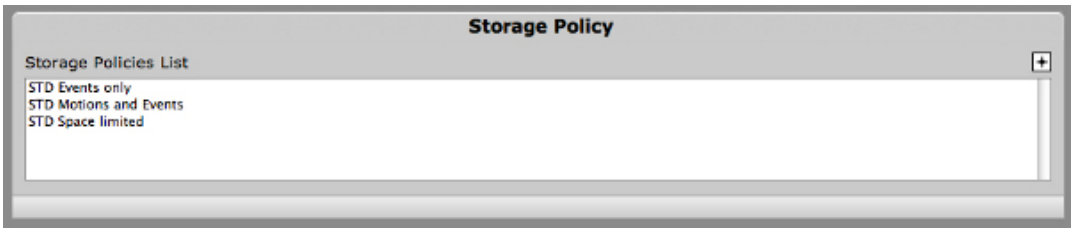


Figure 4.21. Storage Policy

The standard default policies provided when Stratus is installed are:

Table 4.9. Storage Policies

Policy	Description
STD: 24x7 Space Limited	Space consuming devices (cameras, audio) assigned with this policy will record 24x7 and allocate as much storage as is possible and will be recycled when the Storage Manager determines that the amount of free space is below threshold. The threshold is calculated as 5% of the total available space or 3 hours of recording at the current rate, whatever is higher.
STD: Events Only	Space consumers will record only when an Event is created within the context of a particular consumer. Examples of this are Motion Detection events, Analytics events, etc.. The Motion Detector has to be specifically enabled in the “Motion” tab to request the software to analyze the video.
STD: Motion and Events	This strategy is very similar to the “Events Only” setting described above, however the software

Policy	Description
	Motion Detector will be enabled automatically and it will trigger the recording. The sensitivity of the Motion Detector is also different in this scenario: it will trigger the recording for one or more cells, so the “Object Size” setting will be bypassed. This allows for more video in the archives and the ability to perform post-facto searches, where the search region and the object search size is defined at the time of the search, rather than at the time camera is configured. This gives more flexibility at the expense of more storage consumption. This policy will perform recording for any other Event reported, similar to the “STD Events Only”.
STD: No Archive	This setting allows for live view only, with no archive being created for devices with this storage policy. This can be used in conjunction with Schedules to allow turning archive on and off.

Note

Please be advised that “STD Motions and Events” is the policy assigned by default, thus you need to explicitly reassign it if another policy is desired.

All the standard policies are protected from modifications, so you will have to create your own policy by clicking on the “+” icon in the storage policy list header.

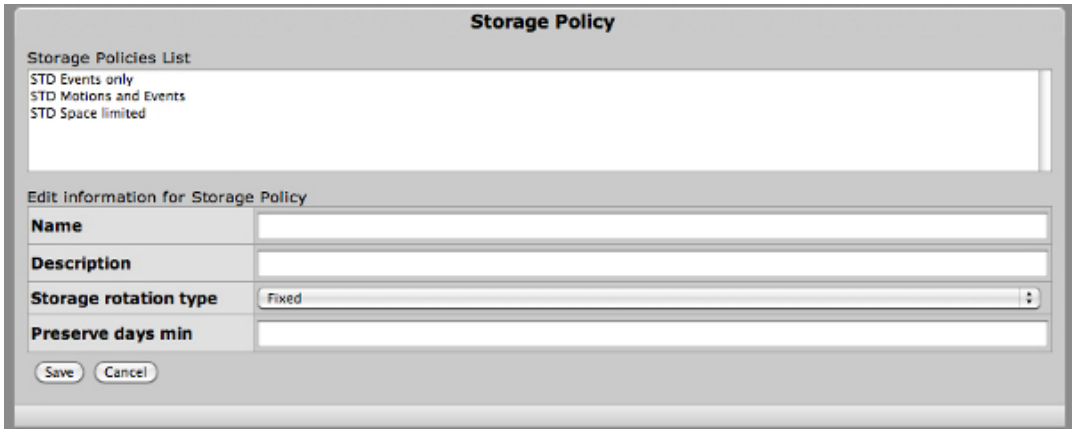


Figure 4.22. Add Storage Policy

After clicking on the “+”, you have the opportunity to create a new policy.

Table 4.10. Timecard

Parameters	Description
Name	Will identify your new Policy when attaching it to the Storage Consumers (cameras), so please keep the name short and descriptive

Parameters	Description
Description	Attribute may be used to explain any necessary details
Storage Rotation Type	This is the most important attribute to consider when creating a Storage Policy. It will affect how much elasticity you allow in your system, and subsequently, how reliable and effective your Storage System will perform. Space limited - This is the default Storage Rotation type and it is the most “elastic”. It will allow the Stratus software to determine how long to store the data based on the amount of storage your system has and its inflow of data. It will keep the minimum reserved free storage space, while maintaining the longest media archive your system can sustain. It is almost impossible to go wrong with this type of storage since it has no additional parameters to configure. Fixed - The most rigid Storage Rotation type. It has a “Preserve days min” parameter to allow you to configure how long (in days) you want your media content to be preserved before it is destroyed. Storage Policy enforcement utilities will delete media content with accuracy of up to one hour (if you configure 1 day to be preserved, it means you will get between 24 and 25 hours of media accessible at any given time). This type of Storage Rotation type is the most rigid one available and it may lead to system misconfiguration by requesting the storage of more data than the Storage System is capable of storing. This may result in a temporary Media Archival stop until some of the older content can be safely deleted. While “Fixed” type usage may be necessary for compliance reasons, we strongly advise that you use it with sufficient reserve in available storage space and/or together with other, more “elastic” types. Range - is a “semi-rigid” Storage Rotation type, which combines the characteristics of both the “Space limited” and the “Fixed” Rotation. It has an additional “Preserve days max” parameter. Storage Consumers using this policy will store at least “Preserve days min” (like in “Fixed”) but will be allowed to store more, but not exceeding “Preserve days max” (similar to “Space Limited”). This Storage Rotation type is the one we strongly encourage you to use, as it offers a limited enforcement (which is required for legal compliance in many cases), while retaining

Parameters	Description
	storage “elasticity”, which may be needed if the storage utilization suddenly changes from expected limits (for example due to temporary unavailable storage Volume or because of increased storage utilization by some of the cameras dues to changes in scene complexity, flow of traffic, etc.).
Preserve Days Min	The minimum number of days to keep storage for. (Fixed or Range only)
Preserver Days Max	The Maximum number of days to keep storage for. (Range only)

Note

Stratus allows the use of multiple Storage Policies, and subsequently, multiple Storage Rotation types in one installation. When multiple conflicting policies compete for storage space, the next set of rules will apply:

- “Cleaner” will remove the oldest media content until sufficient available storage space is achieved (automatically determined by the Stratus software based on multiple factors, approximately 5% of total space)
- Outer limits (“Preserve days min” for “Fixed” / “Preserve days max” for “Range”) will be enforced first and outdated media will be removed permanently
- Inner limit (“Preserve days min” for both “Fixed” and “Range”) will define the limit or the place where the “Cleaner” must stop once the “available storage space” criterion are satisfied
- All the “elastic” ranges will be enforced on “the most fair” approach until the “available storage space” criteria are satisfied. The amount of media content retained will be proportional to the expectations of the Outer Limits, while disallowing Space Consumers with “Space Limited” type to disproportionately increase their space consumption relevant to “Range” type
- When mixing “Events Only” policies with other policies, the Storage Manager will use “the most fair” approach to enforce proportional distribution of storage to these potentially “open-ended” strategies and disallow disproportionate increase of their space consumption over “bound” strategies
- In summary, we recommend that you use one of predefined standard storage policies, which are fully automatic unless you absolutely need to mix Storage Consumers of different importance within one system. The “Event Policy” entity will allow another dimension of reconfigurability to separate more the important information from the general flood of media that your system processes 24x7.

4.6. Configure Event Handling

Event Handling is a very important configuration item, which significantly affects the Storage Management (please see *Section 3.4.1, “Manage Storage Volumes”*).

Events are tags that are preserved in Stratus's database, which provides a convenient way to extract an entry about something that happened in the system at a particular point in time. One of the Stratus

objects, such as a camera or a sensor, registers the event in the system as the “event originator”. The Event may have zero or more “witnesses”, Stratus objects associated to the same event, (such as a camera that can see the same area).

“Events” represent a tag to retrieve information about those events and get the associated media content, such as archived video from the cameras or sound from the audio-devices (which may be the same camera or a microphone on another camera).

There are a few important factors in the concept of Events. The event will have a “lifespan” (age until which it will be preserved), which will protect the media for both the “event originator” and all “witnesses”. If the media content is still protected by the Storage Policy - it will not be specifically deleted when the Event becomes obsolete and gets removed. But, if the Event is getting beyond the point of where the Storage Policy protects the media archive of a particular device from deletion, then the media covered by the Event will be retained until the Event expires and gets deleted. It directly affects the amount of Storage your system will consume. We strongly recommend that you review Chapter 4 on the Best Usage Practices and how to calculate safe and efficient operating limits for your installation.

When an Event gets created in Stratus, it will always be associated to the Event Originator object. Originating objects may be a camera, sensor, relay, or any other type of device that Stratus supports (external devices like Access Control doors or such). The link is established by a device association with a particular Event Policy as shown on the right for the camera configuration editor screen.

To manage the Event Policies, you will have to select “Settings” in the left menu, then choose “Policies”, then select the “Event Policy” option. This action will open the “Event Policy list”, which contains all currently configured Event Policies in Stratus Security Domain.

In the policies list, the “Default policy” is protected from editing, since it is intended to be a system fall-back point, which comes standard with the software and will reliably operate with no additional configuration.

You can add a new policy with the “+” button. To edit the existing policy, click on the policy name.

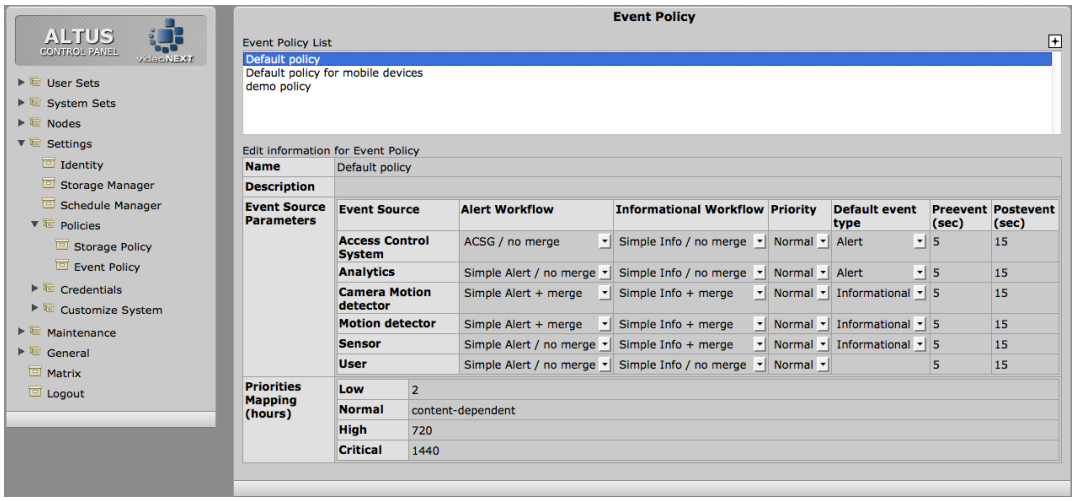


Figure 4.23. An event policy

The Policy “name” should be short and descriptive, since it will be used in a drop-down lists when assigning it to Stratus devices. The “description” may be used to store any kind of additional descriptive information.

The next section of the Event Policy editor defines various parameters for the individual Event Source types. The significance of these assignments is in the automated Event classification based on the Event source. Between these settings only Priority and Lifespan can be altered by the user during the Event life cycle, while the rest are assigned at the time of the Event creation.

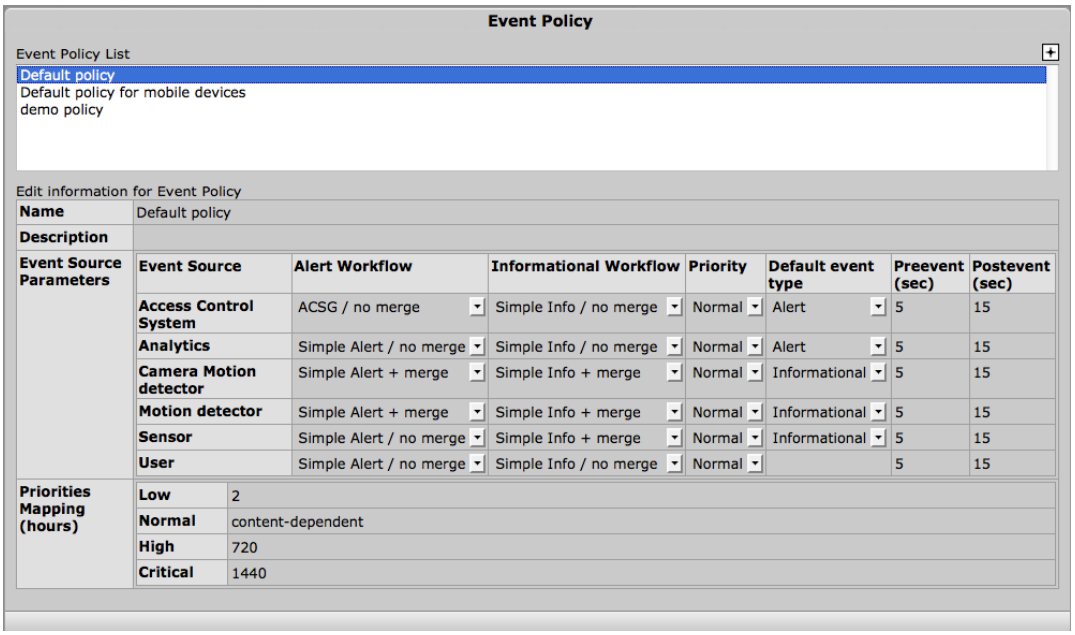


Figure 4.24. Available event policies

Note

Please pay attention to the “Priorities Mapping” section of the Event Policy: it may provide the actual number of hours each Event Priority is expected to be preserved or may be mapped into one of “content dependent” or “space limited” values.

The “Content Dependent” lifespan attaches Event recycling to the recycling of the video content, while “Space Limited” allows content to survive the decimation of non-event video and is managed similar to “Space Limited” Storage Policy (effectively competing for Storage Space).

It is important to grasp the difference between Storage Prioritizing through “STD Events only” / “STD Motions and Events” Storage Policy versus any other Storage Policy in conjunction with the Event Policy based on “Space Limited.” With regard to the Event lifespan, in the first case the video is never written to the Storage, while in the second case the video is stored completely at first and only after that is decimated, which gives the Operator some time (configured by hard limit on Storage Policy) to mark Events and to affect the actual Storage/Events retention. In the first case the process if fully automatic (which is intrinsic, as decision has to be done in seconds) and in the second it requires some user input.

4.7. Configure Sensors

Stratus allows you to register and manage Events from various types of sensor (dry contact, RADAR, etc.), found in the System Set "Sensors", or in a user set the sensor is assigned to:

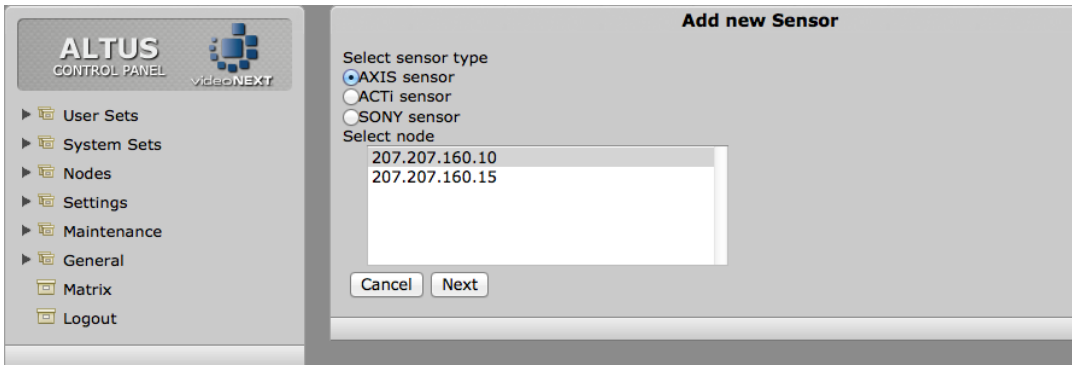


Figure 4.25. Add a new sensor

When you add (or edit) a Sensor, the next dialog will allow you to select the device type and connectivity parameters.

Similar to Cameras, Sensors may be located in any Time Zone, and Stratus presents local device time inside the Events.

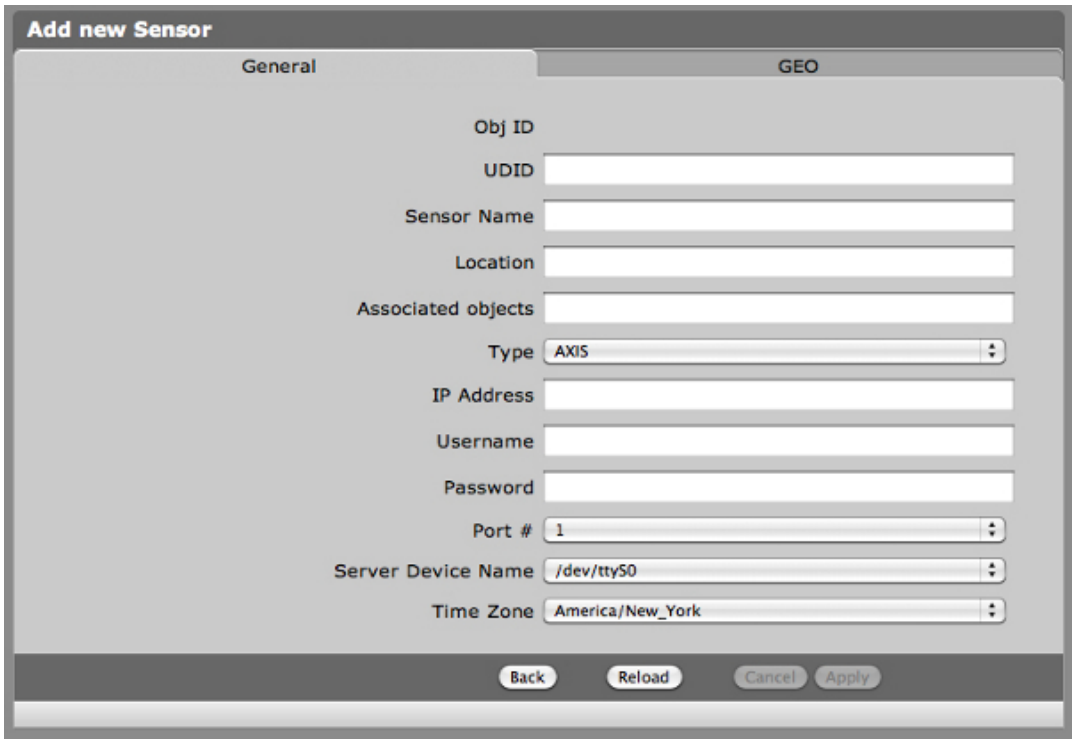


Figure 4.26. Edit sensor

“Associated Camera ID” is similar to “Associated Devices” in Camera’ setting, where it allows the establishment of automated cascading Event propagation from the Originating Object to the Event Witnesses. It allows for automated behaviors like “Camera Popup” or “Audio Notification” to be executed for the associated object (most likely Camera) upon an event registration with a Sensor. While it is optional for cameras, it is used more often for Sensors.

Another method to add cameras is to “Activate” them directly from cameras configuration if a sensor is attached directly to a camera. Click on the "Activate" button in the Camera Configuration->PTZ tab, which will automatically add sensors/relays and will automatically associate them to the camera:

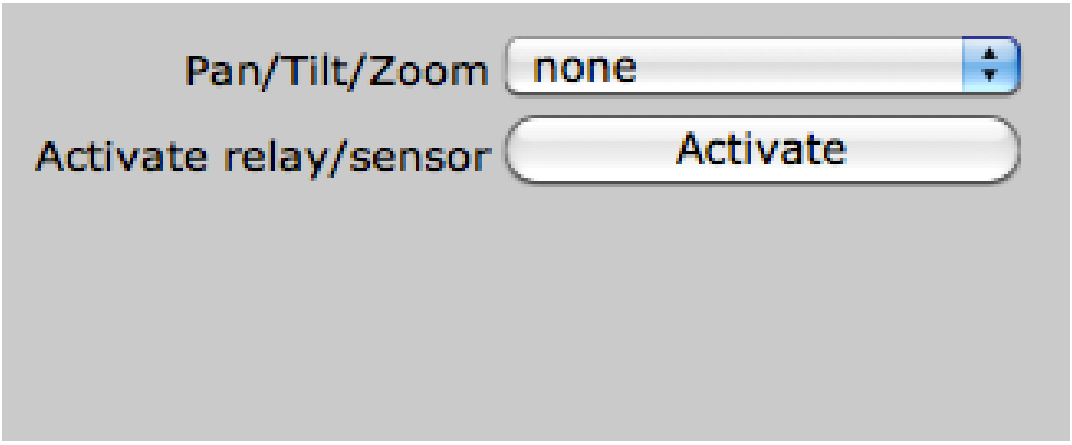


Figure 4.27. Camera Relays

This mode allows the user to automatically maintain the camera-relay/sensor relationship if they are “naturally” associated one to another (by being attached to the same piece of hardware).

4.8. Media Export

The Stratus Operator Interface allows users to export video on-demand to the Operator's computer hard drive (or DVD) without any additional configuration. In addition, Stratus allows the media exported to be on a storage device not directly connected to the Operator's computer, which is useful in cases when Stratus provides the media for other Media Production or Document Management systems like Apple's Final Cut Studio.

By default, Stratus will not have this second functionality enabled until the Administrator configures the data destination directory. To accomplish this, you will have to go to the ““Setting” -> “Identity” in the left menu:

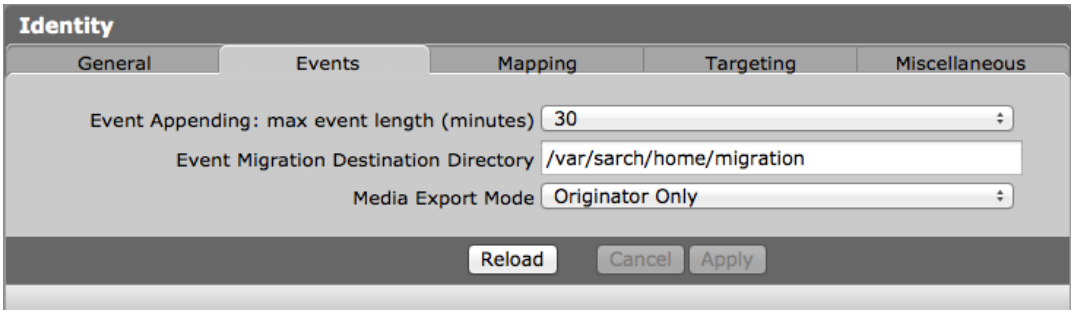


Figure 4.28. Set Export Directory

Note

It is important to provide a resource, which is mounted, but is separate from the OS root directory. The space management is not provided within Stratus and is within the integrator's area of responsibility.

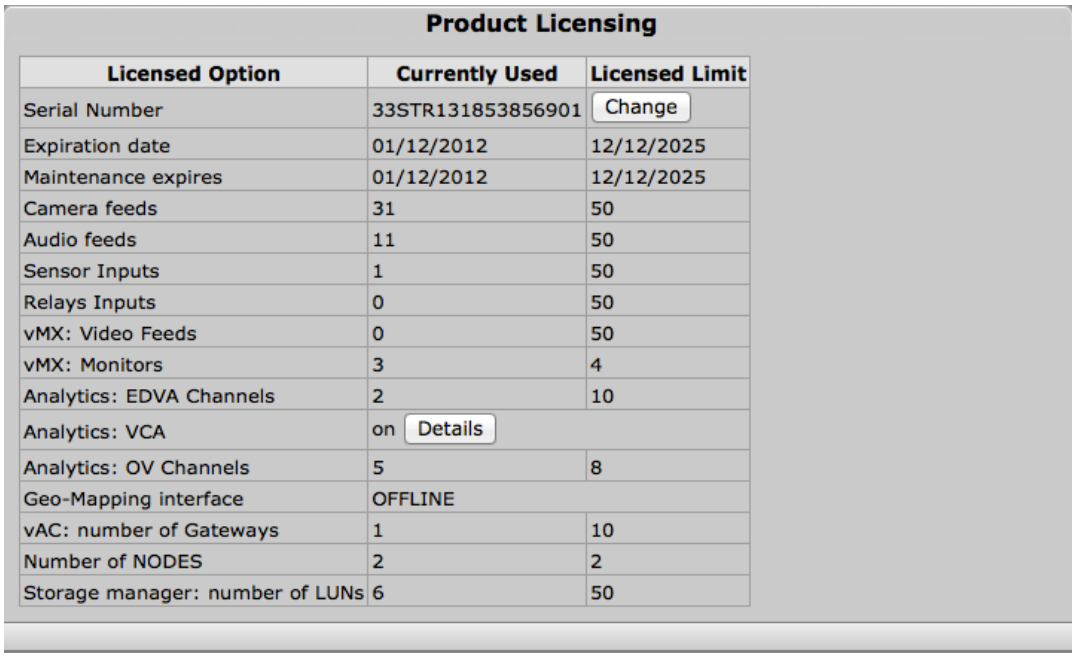
Another important topic associated with media export is “vCrypt” capability, which is the application of a digital signature ensuring authenticity for any exported content leaving the [trusted] confines of Stratus system. Once enabled, all exported video will be cryptographically signed so that the signature can be examined to ensure that the video has not been altered or corrupted. More on this will be covered in *Section 4.12, “Configure vCrypt”*.

4.9. Configure v-MX (Video Wall)

The v-MX (Video Wall) is an option of the Stratus (enterprise edition of the software), but is not available on Cirrus (consumer edition). In this release, v-MX supports an additional control type, VNC Cell, which allows the publishing and sharing of the computer screen on the video wall.

From the deployment perspective, v-MX consists of the server-size functionality, which gets enabled with proper license installation, and additional computers running a “v-MX DS” software package, which turns them into “Display Server Appliances” with no keyboard and mouse. These computers are remotely controlled by Stratus to deliver the Video Wall experience to end-users.

v-MX is a separately licensed software option based on the number of v-MX DS computers to be served and by the maximum number of video feeds simultaneously displayed. Current limitations can always be checked in the left side of Admin Interface in the General->Licensing section.



Product Licensing

Licensed Option	Currently Used	Licensed Limit
Serial Number	33STR131853856901 Change	
Expiration date	01/12/2012	12/12/2025
Maintenance expires	01/12/2012	12/12/2025
Camera feeds	31	50
Audio feeds	11	50
Sensor Inputs	1	50
Relays Inputs	0	50
vMX: Video Feeds	0	50
vMX: Monitors	3	4
Analytics: EDVA Channels	2	10
Analytics: VCA	on Details	
Analytics: OV Channels	5	8
Geo-Mapping interface	OFFLINE	
vAC: number of Gateways	1	10
Number of NODES	2	2
Storage manager: number of LUNs	6	50

Figure 4.29. Licensing limitations

To configure v-MX, you must first configure two devices, a Monitor and a Wall. A Monitor corresponds to the individual monitor-screen, whereas a Wall is a group of monitors.

To add a Monitor click the [+] icon at the top of a set and choose "Monitor", or you can go to the "All Monitors" system set and click [+] there.

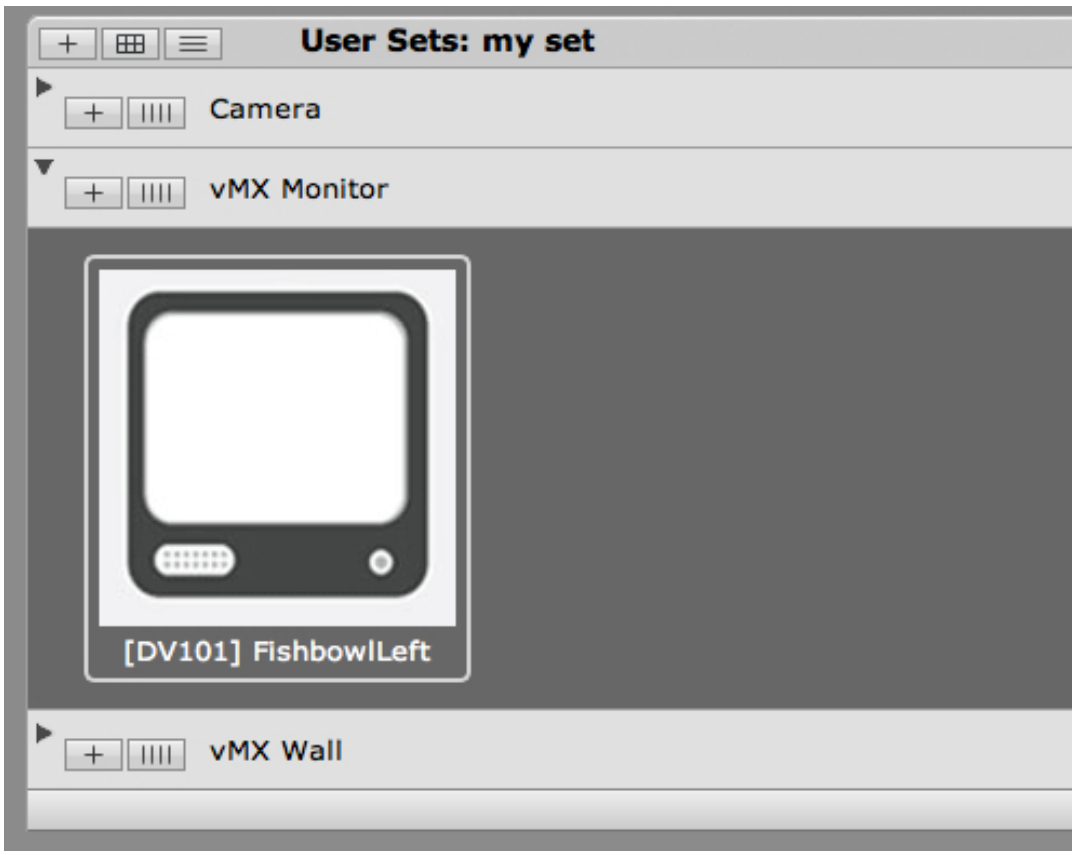


Figure 4.30. v-MX "Monitor"

The next screen is an editor for the Monitor configuration:

Table 4.11. v-MX Settings

Parameter	Description
Obj ID	Unique System Identification for the Monitor. Note this number, as it is needed later. (Read Only)
UDID	User Designated Identifier. If none is provided, one will be created by the system by appending the ObjID to the 'DV' prefix.
Monitor Name	A descriptive name for which monitor this is.
Location	A description of where the Monitor is located. Must not be blank.
TCP/IP Address	The IP Address (or Domain Name) of the v-MX client.
TCP Port	The TCP port to connect to the v-MX with. Recommended to leave on default. Default of port 8510.
Monitor Port	Which monitor attached to the v-MX computer to use (0 is first monitor, 1 is second, etc.)

Parameter	Description
Username	The Username for the monitor. This can be changed with the 'sos' account on the v-MX. Default is 'test'.
Password	The Password for the monitor. This can be changed with the 'sos' account on the v-MX. Default is 'test'.
State	[ON/OFF] - Set whether to use this v-MX on or off.
Status	The current status of the v-MX (like connected, disconnect, etc.). Read Only.

Note

While it is possible to configure v-MX DS to “drive” multiple displays, we suggest using small PCs (AOpen MP45 class) for each individual Monitor. This is more economical, more reliable and has better overall performance.

Once you have your Monitors configured, the next step will be to define Walls:

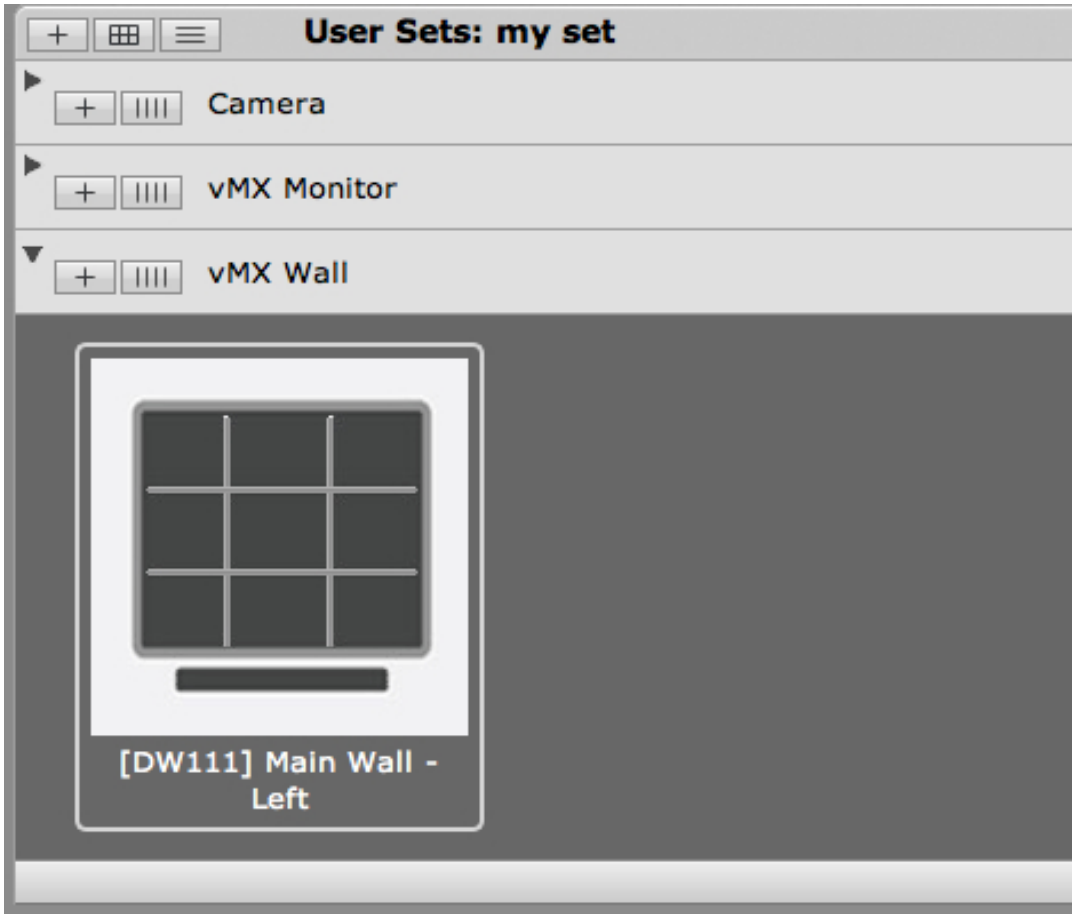


Figure 4.31. v-MX "Wall"

Walls are sets of Monitors arranged into a rectangular matrix by assigning previously created Monitors into cells (as seen above).

The Wall matrix may have empty cells, which accommodates for non-rectangular physical Wall layouts (for example the Wall may have rectangular 3x4 center and “wings” of two monitors on each side mounted around the top, which would be a 3x6 with 4 empty cells).

Different v-MX Walls may be installed in separate rooms and even be geographically dispersed, as long as a sufficient network infrastructure is provided. In general, however, you will want to define a new wall for each logical separation (one wall per each room, or one wall for each operator group in charge of the wall).

Please pay close attention to the “Monitor map” attribute, as it defines a mapping of v-MX monitor IDs into the matrix of monitors representing the video-wall. This "Monitor Map" is a set of triplets defining the position of each monitor. Cell numbering is done starting from 0 (zero), and the triplet format is: row, column, v-MX Monitor ID. Each cell entry is separated by a semi-colon, ";".

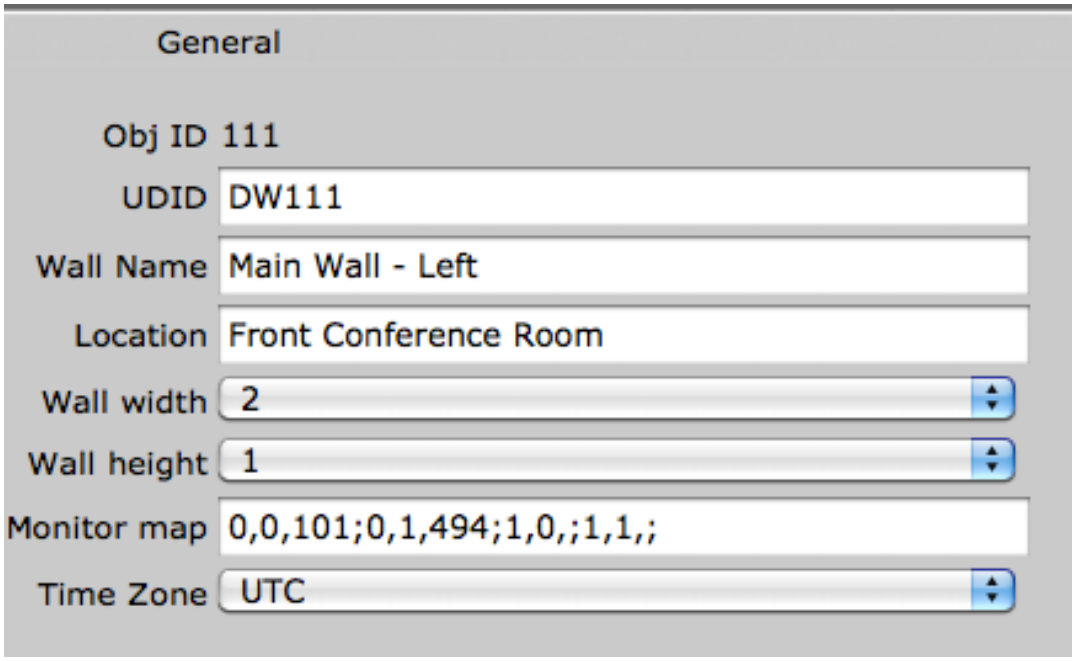


Figure 4.32. Configure the v-MX wall

In the example above, the cell at the top-left (position <0,0>) has the monitor with Obj ID 101, and the monitor at the top-right (position <0,1>) has the monitor with Obj ID 494.

Another important concept of combining multiple Monitors into Walls is the ability to re-combine essentially the same subsets of Monitors into independent walls. It allows sections of the same physical Video Wall to hold different Stratus Roles through the Credential Manager.

The v-MX is effected by Credentials slightly differently than other devices. They will be assigned to Sets, and Sets will be assigned to Roles with permissions. The permissions levels are View, Control, and Manage. Specifically for v-MX:

- View - Does not give any credentials to manipulate Video Wall.
- Control - Allows the recollection of pre-created layouts and manipulation of the monitors (but not to modify saved layouts).
- Manage - Adds the ability to create/edit/delete saved layouts and share them as needed.

For more information on Credential settings, see *Section 4.4, “Users and Roles and Management”*

4.10. Configure v-AC (Access Control)

Stratus allows an external Access Control Systems (ACS) to be made an integral part of the security system sensors and control devices. In essence, it allows the creation of ACS Gateways (ACSG), which are used to automatically discover and describe ACS Objects to Stratus, relay ACS security events into Stratus, and let Stratus call ACS control Methods. ACS Objects are managed as a special set of “External Stratus Objects”, but allow the application of a uniform set of Credential Management and processing rules in the fashion uniform to the rest of Stratus Devices.

There are multiple commercial ACS vendors on the market, and Stratus defines a universal layered Stratus ACSG API. videoNEXT offers a number of ACSG software integrations as an add-on to the standard Stratus package. If such an add-on is not developed it usually requires only a moderate effort on the integrator side to create one. Please inquire for more information from your Vendor.

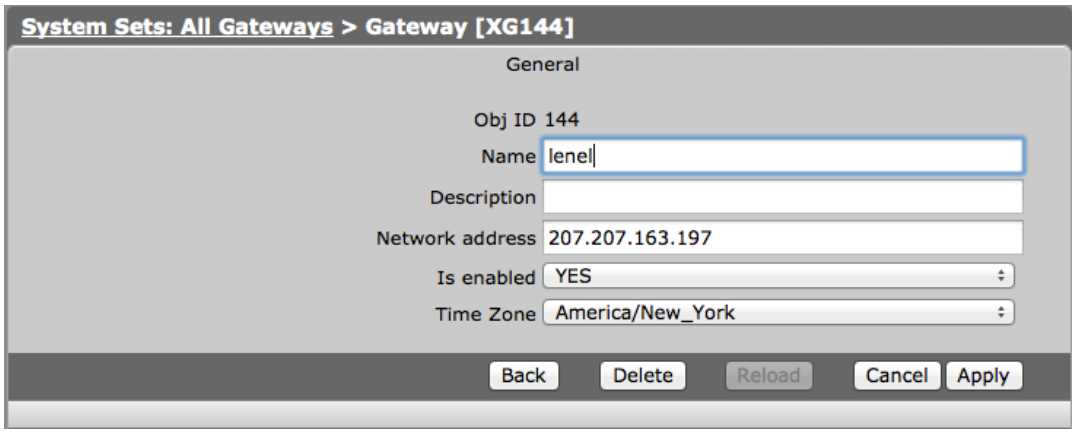


Figure 4.33. Access Control Gateway

Initially, you will have to create a Gateway in the “Manage Gateways” screen and configure “Obj ID” into ACSG product specific for your particular ACS - it will be used for Stratus handshake procedure.

Once you enable ACSG product to communicate to your ACS, Stratus will receive a full list of devices, which will be presented into the Gateway you created on the initial step. You will have to identify and enable ACS objects you will want Stratus to communicate with by clicking on the device icon in the list and changing “Is Enabled” option to the “yes” value.

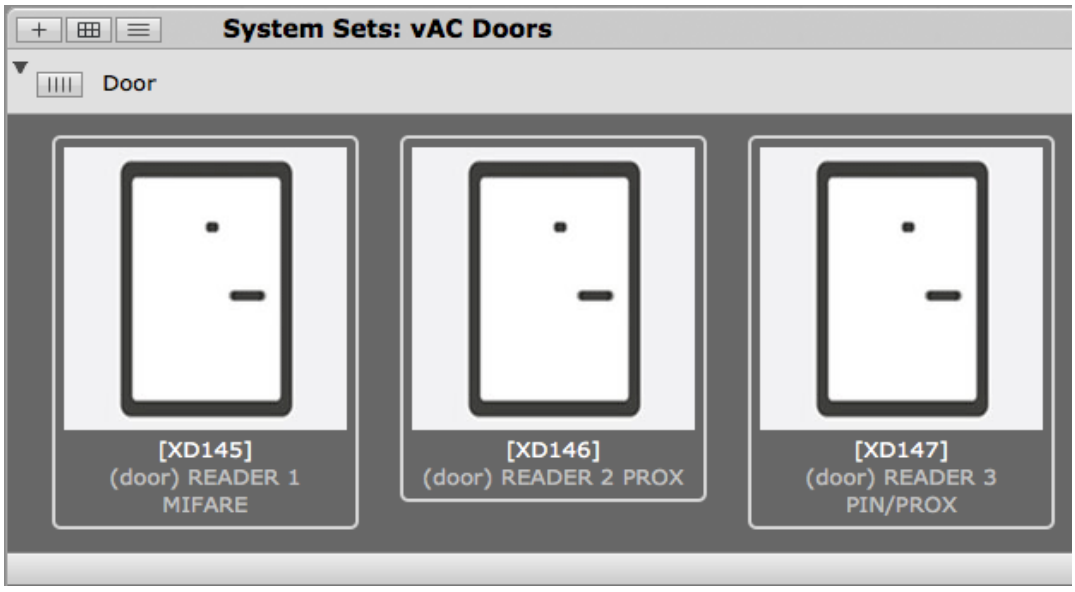


Figure 4.34. A door Device

Once you are finished with basic ACSG configuration, the list of devices will be presented into the Credentials Manager screen for assignment and permissions management. The Credentials Manager is described in greater details in *Section 4.4, "Users and Roles and Management"*.

4.11. Schedule Manager

The Scheduler has been refactored and expanded in Stratus 3.3. Schedules can now be created as system-wide objects, and then assigned to individual Cameras.

The Scheduler is a system-wide set of Policies, which are established in one place and then are used by any camera device in the system. This design consideration significantly simplifies system deployment and maintenance.

The Schedule creation and modification process was simplified with scheduler user interface in "Control Panel", similar to one used by Google Calendar. It allows the administrator to define multiple individual and repeating time intervals and associated System Posture settings, which control the most important settings like Device State (on/off), Storage Policy, Motion Detection, etc... The Schedule policy has an important concept of the Default Posture, which defines which individual setting[s] will be controlled by the Schedule and their default values. Once a Schedule is assigned to a certain device, it takes over (overrides) listed parameters' maintenance (in other words, old values of these settings on device-configuration have no effect and are disabled, since now the Schedule controls it). This allows for relative ease of system administration and maintenance, especially for installations with tens and hundreds of devices.

You can access the Schedule Manager by clicking 'Settings->Schedule Manager'.

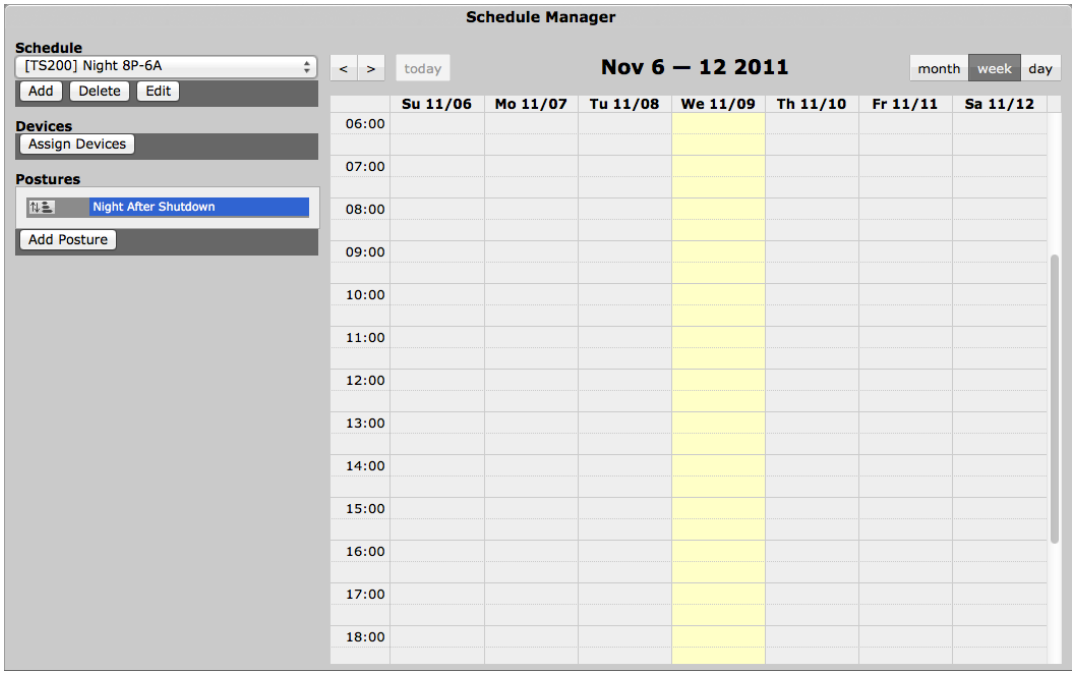


Figure 4.35. Schedule Manager

4.11.1. The Schedule

To add a schedule, click the Add button under "Schedule" in the upper left. To edit a schedule, select the schedule then click the Edit button. Both options will open a window that looks like:

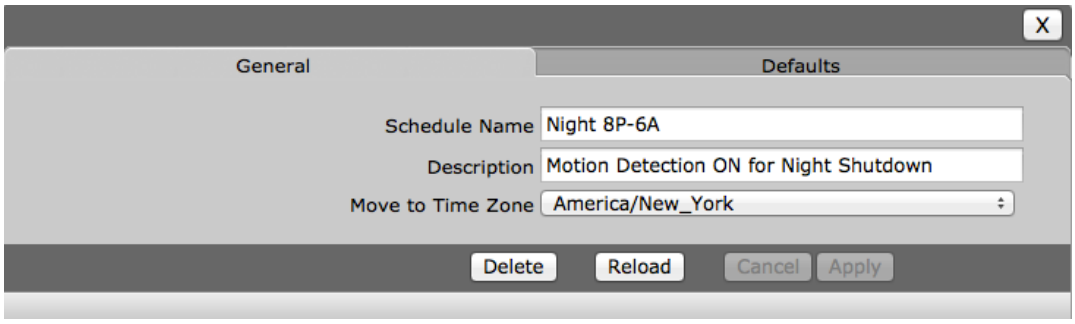


Figure 4.36. Schedule General

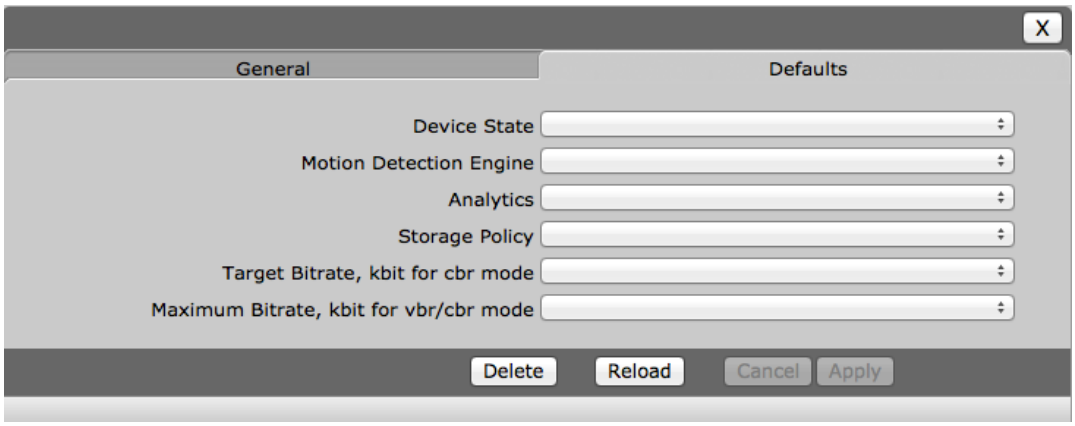


Figure 4.37. Schedule Defaults

On the General tab, you can set the Schedule's Name, give a brief description for it, and set which timezone it should operate in.

The Defaults tab sets what this schedule controls. The schedule will only be able to control attributes which have a default set on this page.

Table 4.12. Schedule Defaults

Parameter	Description
Device Status	If selected, sets the default state of the camera to on or off.
Motion Detection Engine	If selected, sets the default state for Motion Detection to on or off.
Analytics	If selected, sets the default state for Analytics to on or off.
Storage Policy	This is a list of available Storage Policies. If selected, sets the default storage policy.
Target Bitrate	(in kbps) If the camera is in variable bitrate, this option sets the default targeted bitrate.
Maximum Bitrate	(in kbps) If the camera is in constant or variable bitrate, this option sets the default Maximum bitrate.

Important

Once a default is chosen and cameras assigned, it is no longer possible to control that setting in the standard camera interface.

Once configured, click Apply to add (or finish editing) the schedule.

4.11.2. Postures

The next step is creating *Postures*. A Posture is a what state to change a camera to, from the default, based on the time. For example, you can set a posture to turn Motion Detection on at night, when the default (set in the Schedule) is for Motion Detection to be off. Postures created as a sub-entity to schedules, so each schedule can have its own set of postures that are not shared. A list of all Postures is shown on the left of the Schedule Manager screen.

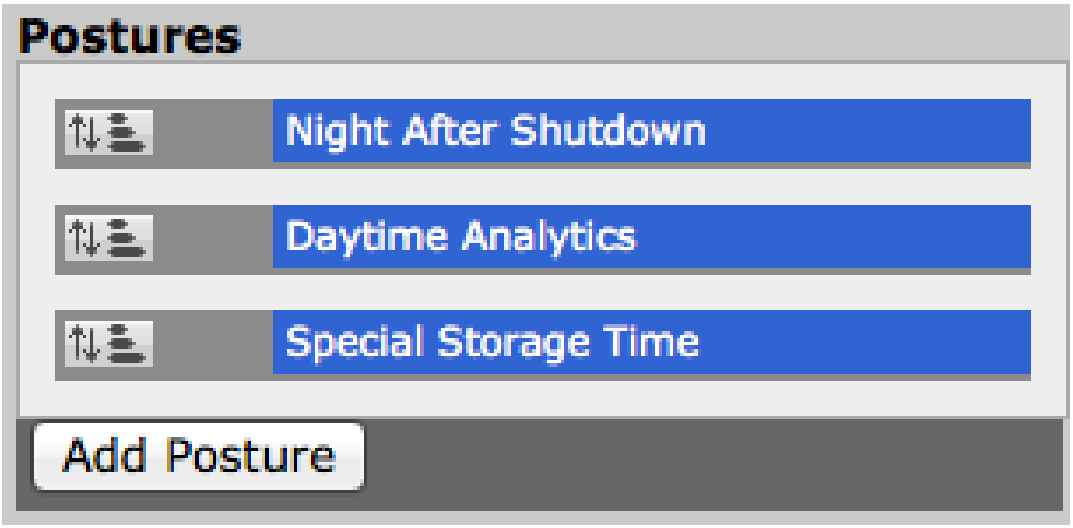


Figure 4.38. Postures

The order in which Postures are displayed dictates their priority, in the case of a conflict; the higher on the list, the higher the priority. To rearrange priority, click on the will allow you to drag the Posture up or down to re-prioritize it.

Clicking on a Posture will allow you to edit it. Clicking on "Add Posture" will allow you to create a new Posture.

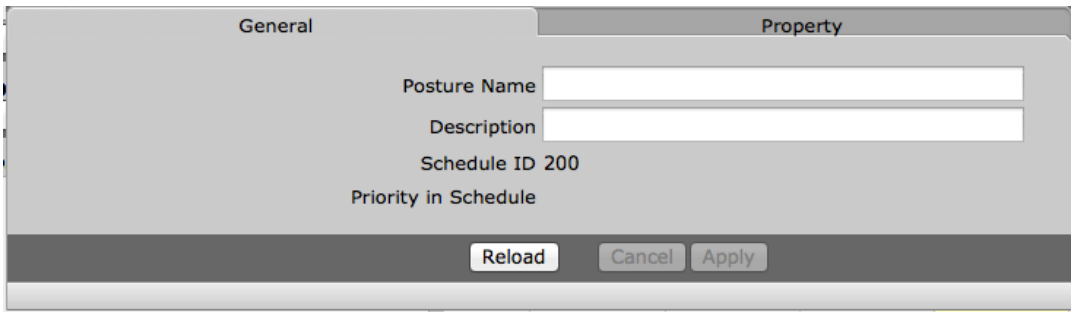


Figure 4.39. Posture General

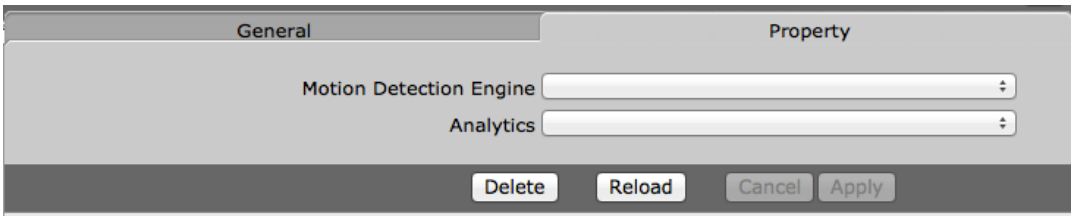


Figure 4.40. Posture Property

The General tab will allow you to set the Posture name, and give a brief description.

The Property tab will allow you to set changes from the defaults that were chosen in the Schedule. The only options that will be displayed are those that have defaults set in the Schedule. For example, you can set Analytics to OFF, when the default state is for them to be ON, then whenever this Posture is applied the Analytics will be set to off, and whenever the Posture is not in effect Analytics will be turned back on.

4.11.3. Scheduling a Posture Timecard.

Posture *Timecards* can be scheduled by dragging a Posture to the calendar. This interface is very similar to the one use by Google Calendar. All timecards will be displayed as spanning the time for which they are set, and multiple timecards will be displayed at once.

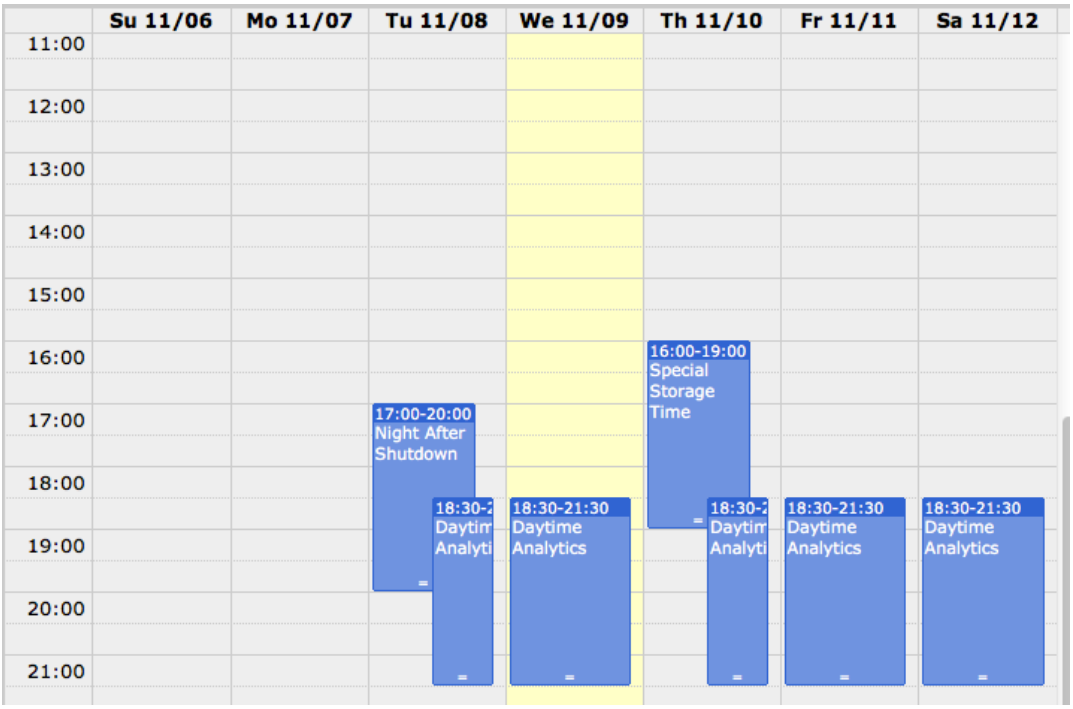


Figure 4.41. Scheduling a Timecard

When a Posture is scheduled, it will default to show covering three hours. To change the time period, add a special name/description, or to set the Posture to repeat, click on it to open an editing window.

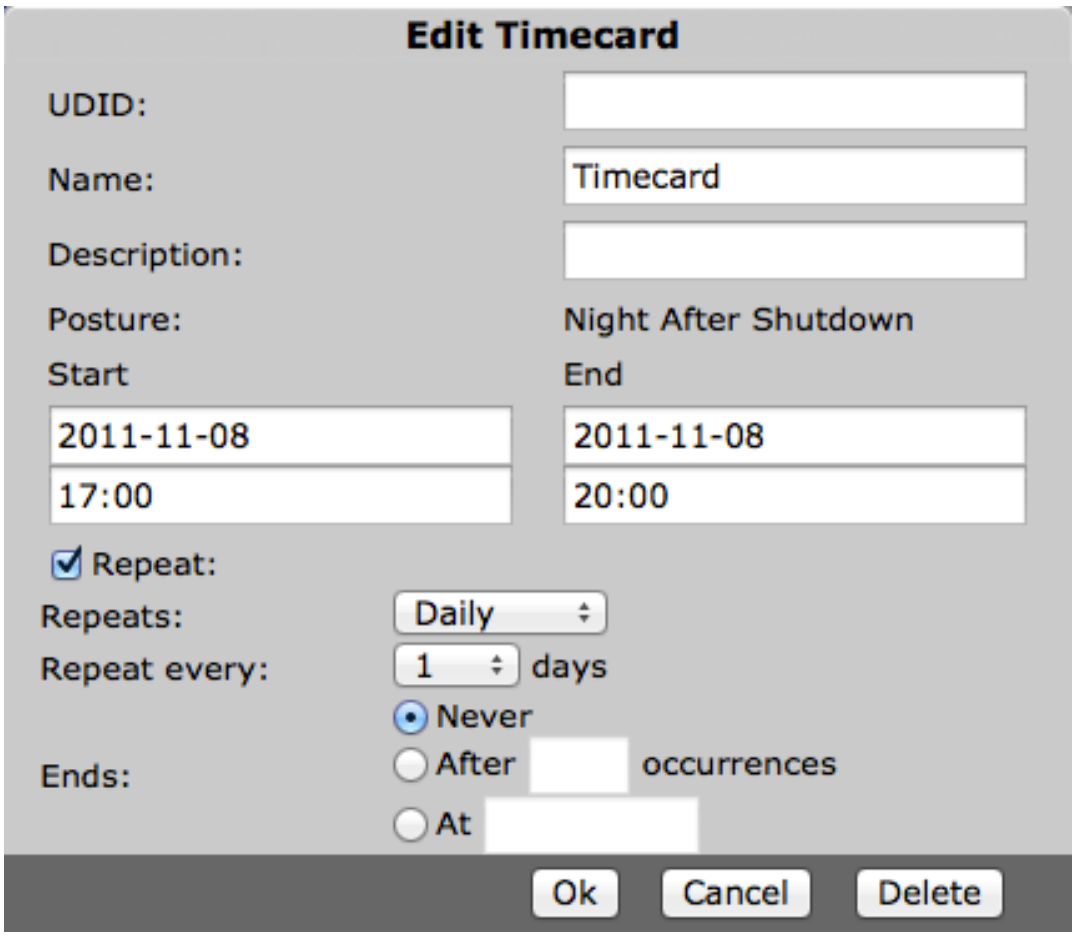


Figure 4.42. Edit Timecard

Table 4.13. Schedule Timecard

Parameter	Description
UDID	User Defined Identifier - You can give this Timecard a unique identifier if desired. (Optional)
Name	Some Name for the Timecard.
Description	A brief description of the timecard. (Optional)
Posture	Which Posture this Timecard belongs to. (Read Only)
Start	These two fields are for Date and Time to start this timecard. • Date - Clicking the Date field will open a calendar to select the date. • Time - Clicking the Time field will open a selector to choose the time.
End	These two fields are for Date and Time to stop this timecard. See "Start".
Repeat	Select to allow the schedule to be repeated.

Parameter	Description
Repeats	[Daily/Weekly/Monthly] - Select the frequency the timecard should be repeated.
Repeat Every	Allows scaling of repeat interval, for example setting to "2 days" will repeat every other day.
Repeats On	(Only shown for Weekly) - Sets which day of the week this timecard will repeat on.
Ends	Sets when to stop repeating. Never - never stop repeating After X Occurrences - Set to stop repeating after X times. At X - Sets to stop at the chosen calendar date.

Once the timecard is configured, hit OK to save changes, Cancel to cancel changes. Press Delete to remove that timecard and all repeats of it.

4.12. Configure vCrypt

Cryptographic signatures are used to guarantee the authenticity of video-clips exported from the secure environment of the Stratus system. Once enabled, Stratus automatically places a verification signature on any video-fragment leaving the confines of the system. Modern, industry-standard cryptography is used to guarantee the authenticity of both the signature and associated signed-video. Even the smallest (one-bit) alteration of the content is guaranteed to be reliably detected by this algorithm.

vCrypt comes as a standard capability inside the Stratus software. vCrypt is built upon the public/private key infrastructure. Upon software installation Stratus will generate a unique key pair.

Note

The public/private key pair may be regenerated if needed.

The key must be kept well-protected and preserved. For this reason it is not a part of the Configuration Backup, nor the Support File creation and should be safeguarded by the System Administrator as a separate configuration item.

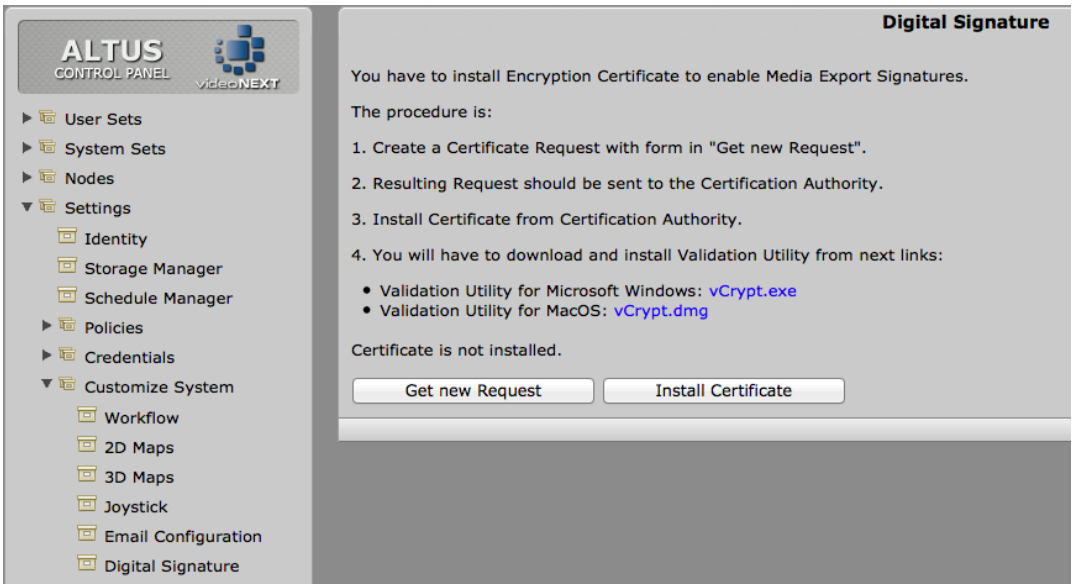


Figure 4.43. Configure vCrypt

Established and trusted Certificate Authority (CA) would be needed to create a certificate, which will be used to sign all the digital content.

To configure the vCrypt functionality, you have to open the Operator Panel and go to Setting->Customize System->Digital Signature. The necessary steps are detailed on that page.

Once you finish installing a digital certificate, all media exported from Stratus will receive a digital signature automatically. Special "vCrypt" utility is used to confirm the exported media content's authenticity. It may be downloaded as a Windows executable directly from Stratus Admin Interface on the Digital Signature page.

The Validation utility requires the Certificate file to validate content authenticity. It is SAFE to export and share the Certificate file, as it cannot be used to derive your encryption key.

Suggestions

This section is for various suggestions and metrics for deciding hardware, network, and storage capacity required.

5.1. Recommendations on Client Station platforms

PC/Windows platform, minimum requirements:

- Screen resolution of at least 768x1024. Resolution of 1024x1280 or higher is recommended.
- Intel Core 2 or newer system with at least 2 GB or RAM and decent video-card.
- Multi-core CPU is strongly recommended if you expect to open more then 4 or 5 videos simultaneously.
- Internet Explorer 8 or Google Chrome web browser.
- Java Run-time 1.6 update 22 or newer.
- Adobe Flash Player 9 or newer.

For Internet Explorer browser we strongly recommend setting your cache size to 40-50 Megabytes (down from default size) to prevent the browser from degrading your computer performance. As an extra precaution, you might also need to set the browser cache settings to “Update cache upon every visit to the page” in the “Internet options” if you experience any unexpected UI behaviors.

Apple Macintosh platform minimum requirements:

- Screen resolution of at least 768x1024, 1024x1280 or higher is recommended.
- Intel CPU based Macintosh with at least 1.4 GHz CPU and 2 GB or memory (older PowerPC CPUs are not supported).
- Safari web browser. At this time, it is recommended to keep the Safari version from updating to 5.1.
- Up to date Snow Leopard or Lion OS with all updates installed.

Troubleshooting

This section describes the Security System troubleshooting. The main goal for videoNEXT is to make sure our customers have their systems reliably working 24x7 and that problems, if any, are resolved in a fast and efficient manner without disrupting the operations.

videoNEXT offers various Support options, which are different in the expected response time and types of incidents covered.

In any case, the first level of troubleshooting should be done before contacting your Integrator or videoNEXT Support, as it mostly involves initial information gathering and basic analysis.

6.1. How to Identify and Classify the issue

The first and most important step in getting specific issues contained is to Identify and Classify. In essence, in this step you have to identify which part of your Security System is at the root of the issue and define your Plan for the resolution.

The first place to consider is the “network”, as this is a blood line of your Security system and it will not function without it. If the Operator's station normally has access to the Internet and will not now allow access to major sites like Google or CNN, then the “Network”, the connection, or the network is a very likely the reason for your Security System issues. Contact your Network Administrator and resolve the issue before continuing further with the troubleshooting. If the Operator station normally has no access to the Internet, you can check the connectivity to the internal network resources to make similar determinations.

Once you ruled out the Network as a possible cause of the problem, the next step will be to determine if the problem is with the “client station versus something else”. At this step you are trying to contain the problem to a particular Client Station by testing essentially the same functionality on another computer. Try to open the browser and point it to the Security System from another workstation. If another computer has no problem, then you can conclude that the Client Station is the route of the problem and proceed with troubleshooting accordingly.

If these first two causes were disqualified, you may assume that problem resides in the Stratus’ server[s].

Please make sure to follow the procedure in *Section 6.4, “Documenting Software Issues and Getting Support”* when filing support request.

6.2. Issues with Client Station

Normally, Stratus does not require any special installation on the Client Station other than software dependencies like a Web Browser, Java and Flash Player. Please make sure your computer has the proper versions of these components (see *Chapter 5, Suggestions* for details).

A general note on the client platform is that browser-based clients are as stable and reliable as the browser itself. Browsers may freeze or crash frequently for any type of web-application, and Stratus is no exception. You may expect to get a sufficiently stable operation from commercial products like Microsoft Internet Explorer on a Windows PC or from Safari on Apple's Mac OS X, while popular alternatives like Google Chrome or Mozilla FireFox are less stable in general.

It is always beneficial to check if the problem is related to your unique computer or it is consistent on any other computer you may have around. This allows you to easily distinguish between a Stratus problems and a computer/OS problems. This is an important quick-test which you should not overlook,

as explaining your situation to support will take time, and the first troubleshooting step will be the very same, so you will save time if you come prepared.

If you experience a problem with you browser-based Stratus client, please follow the next steps to get back to normal operations:

1. The fastest resolution is to “Reload” your browser (associated to the F5 function key or Ctrl-R on keyboard for most of platforms). It resolves issues in 95% of cases.
2. If the issue is still not resolved, please try the next, and more elaborate, procedure:
   a. Close all browser windows (plus make sure the browser was shut down in Dock on OS X).
   b. Start the browser once again, but do not open Stratus software yet.
   c. Clean browser cache:
      - For Internet Explorer - “Tools->Internet Options->Browsing History->Delete..->Temporary Internet Files->Delete”.
      - For FireFox - “Tools->Clear Private Data->Clear Private Data”.
      - For Safari - "Safari->Reset Safari".
   d. Open Stratus application once again, and recheck.
3. Clear Java cache:
   - Windows - Go to Control Panel. There you can open Java preferences. Click "Delete Files" in the Network tab..
   - Mac OS X - Go to Application->Utilities->Java Preferences. Click "Delete Files" in the Network tab.
4. As a final resort for the most stubborn browser-related problems, you can try to reboot your computer.
5. If it still does not work - you may need to request Support.

Please make sure to follow procedure in *Section 6.4, “Documenting Software Issues and Getting Support”* filing support request.

6.3. Issues with Stratus Server

The Stratus server software is specially designed to automatically resolve the problems that can be fixed without administrator intervention. This includes recovery from inconsistent situations on storage, cameras, connectivity, etc...

The information below outlines the most common scenarios of how the Administrator can use the tools provided by Stratus to go beyond the automated recovery process and actively look for clues to resolve the situation when Stratus does not automatically recover.

6.3.1. Camera does not retrieve video

The first step in the “no video” troubleshooting will be to confirm that the camera itself works. Most cameras have their own interface for viewing video directly from the camera. If your camera supports this, you can follow the following steps to narrow down if the server or the camera is likely at fault:

1. Go to the camera configuration of Admin Interface and identify the camera IP address in the “Source” tab of the configuration screen.

2. Open an additional browser window with a camera the native interface using that address as the URL.

- If the camera does not work in a native camera interface, then troubleshooting should be performed on the camera itself (network, power, device was disconnected, stolen, etc..).

- Otherwise, further investigation into the Stratus Camera Configuration screen should be performed.

The next step will be to check if the camera's Username and Password are properly configured in the Stratus Camera Configuration screen. An attempt to connect to the camera directly may be used to validate the Username and Password. It is usually done in the “Setup” section. Reset the password in the Stratus camera configuration to the known good one before proceeding further.

If the previous steps did not resolve the issue, you can view detailed log information for the camera in the Camera Editor:

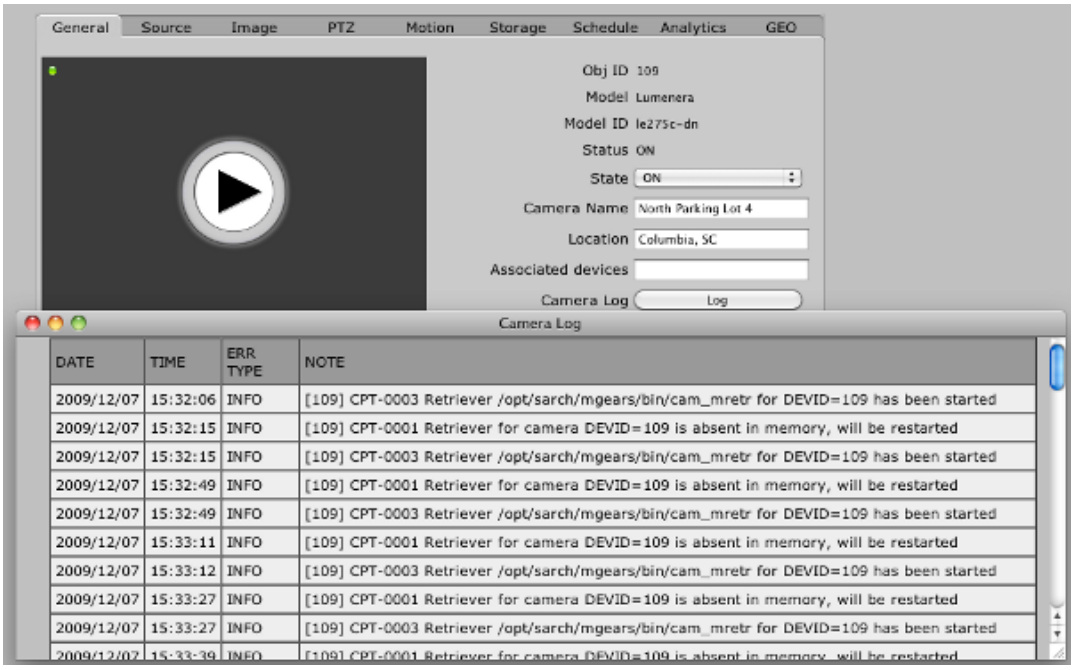

General
Source
Image
PTZ
Motion
Storage
Schedule
Analytics
GEO
Obj ID 109
Model Lumenera
Model ID le275c-dn
Status ON
State ON
Camera Name North Parking Lot 4
Location Columbia, SC
Associated devices
Camera Log
Log
Camera Log
DATE
TIME
ERR TYPE
NOTE
2009/12/07 15:32:06 INFO [109] CPT-0003 Retriever /opt/sarch/mgears/bin/cam_mretr for DEVID=109 has been started
2009/12/07 15:32:15 INFO [109] CPT-0001 Retriever for camera DEVID=109 is absent in memory, will be restarted
2009/12/07 15:32:15 INFO [109] CPT-0003 Retriever /opt/sarch/mgears/bin/cam_mretr for DEVID=109 has been started
2009/12/07 15:32:49 INFO [109] CPT-0001 Retriever for camera DEVID=109 is absent in memory, will be restarted
2009/12/07 15:32:49 INFO [109] CPT-0003 Retriever /opt/sarch/mgears/bin/cam_mretr for DEVID=109 has been started
2009/12/07 15:33:11 INFO [109] CPT-0001 Retriever for camera DEVID=109 is absent in memory, will be restarted
2009/12/07 15:33:12 INFO [109] CPT-0003 Retriever /opt/sarch/mgears/bin/cam_mretr for DEVID=109 has been started
2009/12/07 15:33:27 INFO [109] CPT-0001 Retriever for camera DEVID=109 is absent in memory, will be restarted
2009/12/07 15:33:27 INFO [109] CPT-0003 Retriever /opt/sarch/mgears/bin/cam_mretr for DEVID=109 has been started

Figure 6.1. Camera Log

This tool will allow you to see the exact sequence of events and how a camera is getting recognized and started in Stratus’ internal service processes. You can look for information suggesting there is a network issue, or invalid username/password configured. In particular, look for Warning, Error, or Fatal types of log entries. The issues reported here are a direct diagnosing tool when investigating why a camera does not work.

The next step in the camera configuration analysis will be to check that the individual settings are not contradictory:

- If the camera uses H.264 or MPEG4 codec: please make sure that the “target bit rate” is not set to be higher then “maximum bit rate”, as some cameras will stop video streaming with such parameters settings

- Setting the resolution to the high settings and bandwidth to overly low settings may prevent some encoders from producing a stream. Try increasing the allowed bandwidth and/or reducing the resolution and checking the results

- For most cameras, MJPEG codes will be used with HTTP protocol over port 80, while H.264 and MPEG4 will be used with RTSP protocol over port 544. Other combinations might not work. Camera editor will try to shield the installed cameras from such mistakes, but they are still possible.
- If Stratus has no storage in an accessible/writable state or if you are using a “motions-only” type of storage policy, the camera will perform “live streaming”, but will have no video-archive

6.3.2. Camera PTZ does not work

The most likely reasons for problems with camera PTZ control are:

- Camera does not support PTZ. Check if your particular camera model supports PTZ controls.
- The PTZ protocol is not properly set in the Stratus camera configuration. Check on the “Controls” tab in the camera configuration editor.
- The PTZ driver is not loaded into your Video Server (encoder). This confusion is common for the novice Axis equipment users, connecting analog cameras to Video Servers (models 241, 7404, etc..). You have to select “Axis” as a protocol for the Stratus PTZ, but in addition you have to load the appropriate PTZ driver into your Axis Video Server for you particular camera model. These drivers are available for download from the Axis web site upon registration
- The Camera ID is not properly set in the Stratus configuration. If you have a multi-port encoder with multiple cameras connected, usually it is the port ID on the encoder.
- If you use ICD001 or PTCRxx types of PTZ protocols, make sure to select the PTZ driver that corresponds to the device protocol, and configure TCP Port settings to the appropriate value to talk to the Pan-Tilt controller

6.4. Documenting Software Issues and Getting Support

Depending on how the system was installed, it is very likely that our Reseller Partner or Integrator will be responsible for the first level of support (underlying hardware and/or system software) before the problem is classified as a software issue and gets reported to videoNEXT per the Reseller Agreement and/or Maintenance and Support Agreement.

In the majority of cases, your Integrator or Reseller will be a proxy in getting proper resolution for your problem[s], as it may involve coordinations between various vendors, which were involved in your unique setup.

We strongly encourage you to perform the basic internal troubleshooting before requesting Support. You will need to perform some information collection and basic triage and will be able to resolve your problem much faster having done so. If the problem is not trivial, our Stratus Reseller or your Integrator will be happy to help you resolve it, and the information you collect during initial the troubleshooting steps will make it more expedient.

When contacting Support, please collect the following information before you call:

- Precise description of problem(s) you experience: what you see, and what you expected to see. Is the problem repeatable?
- Please specifically emphasize your primary concern(s), while listing the rest of the issues as secondary.
- Your system serial number (can be found in “General->Licensing” page)

- Please collect the “Support File” (can be created in “Maintenance->Support Files” page) as soon as possible. It will give a Support person much more internal information on what was happening in the system when the issue occurred. This information is constantly recycled, so it is important to retrieve it quickly after the problem occurred. For severe problems, it may be lost even after few hours, as the amount of cyclical storage space is limited and a flood of error messages may obscure the original issue, making the root cause identification hard, if not, impossible.

Appendix A. Analytics

videoNEXT Stratus is designed to accommodate multiple analytics algorithms: both embedded and external. Stratus Release 3.3 includes the support of two algorithms for object behavior analysis and display in real-time:

1. The VCA algorithm, either software-based or utilizing hardware-based acceleration on edge devices supporting it (UDP, videoNEXT, Dante). This option requires either hardware that supports this, or a software license.

2. The Object Video algorithm is a high-quality algorithm. Its performance is very good, and there are more complex behavior rules so that alarms will only occur on very specific situations, if desired. It is, however, a more expensive option.

At the outset a cautionary note is in order regarding the processing power required to run the Analytics on Stratus. Analytics algorithms by their very nature are resource intensive. This should be kept in mind when enabling analytics on multiple cameras. It is advised that the user's requirements regarding analytics, the corresponding hardware processor resources are carefully planned and employed to get good performance. Get in touch with the videoNEXT Account Manager to get engineering support as necessary.

The next step is to establish the Behavior Analysis configuration. Stratus 3.3 supports internal Behavior analysis inside the software (one of the SSVA options) and in addition it allows the performance of behavior analysis on the edge for hardware supporting VCA analytics (EDVA, supported on some hardware). For edge-based behavior analysis, you will have to connect to the edge device's interface and configure the analytics behavior there directly.

A.1. Types of Tracker Rules

To open the tracker configuration, click the "Configure" button in the analytics tab for the camera. This will open an overlay. In one half of the screen will be the zones and lines you have created overlain on the video.

The other half displays the various rules, behaviors, filters, and additional settings specific to the algorithm chosen. A dropdown menu allows you to select Zones and lines that you have already configured. The buttons below allow you to add new Zones or Lines, or delete the currently selected Rule.

There are two main types of rules: zones and tripwires. Additional filters and behaviors can be applied to each of these rules to form complex alert conditions.

Briefly:

1. Zones - Zones are regions in which various rules may be applied. These rules include things like Enters, Exits, Presence, Loiters, Object Taken, or Object Left Behind. Zones are drawn as polygons, starting out as a square.

   To add additional corners, double clicking on an edge. To reshape, drag a corner. To move the zone, drag from the center.

2. Lines - Lines enforce rules only on the threshold of when an object crosses them. They work as virtual tripwires and can enforce both one-way and two-way traffic, and discriminate based on size or classification.

   To add additional "joints", double click on the a line segment. To reshape, drag any end point or joint. To move, drag from a line segment.

While the interface for configuring behavior for both SSVA (Software-Side Video Analytics) are very similar, there are enough differences that they will be covered in separate sections below.

A.2. VCA Tracker Configuration

The VCA behavior can be configured with either Lines or Zones. There are additional tabs for configuring Channel Settings, Classification, or VCA Calibration. The following sub-sections will go in to more details about each.

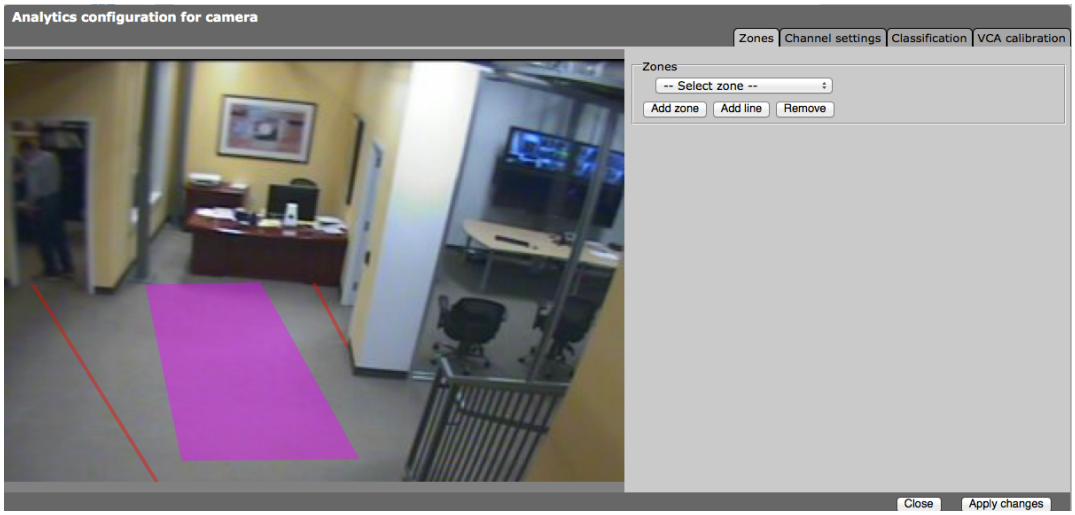


Figure A.1. VCA Analytics Rules

A.2.1. VCA - Adding and Editing Zones

If you click the "Add Zone", a small Zone box will be displayed in the video, and additional configuration options will be displayed on the right.

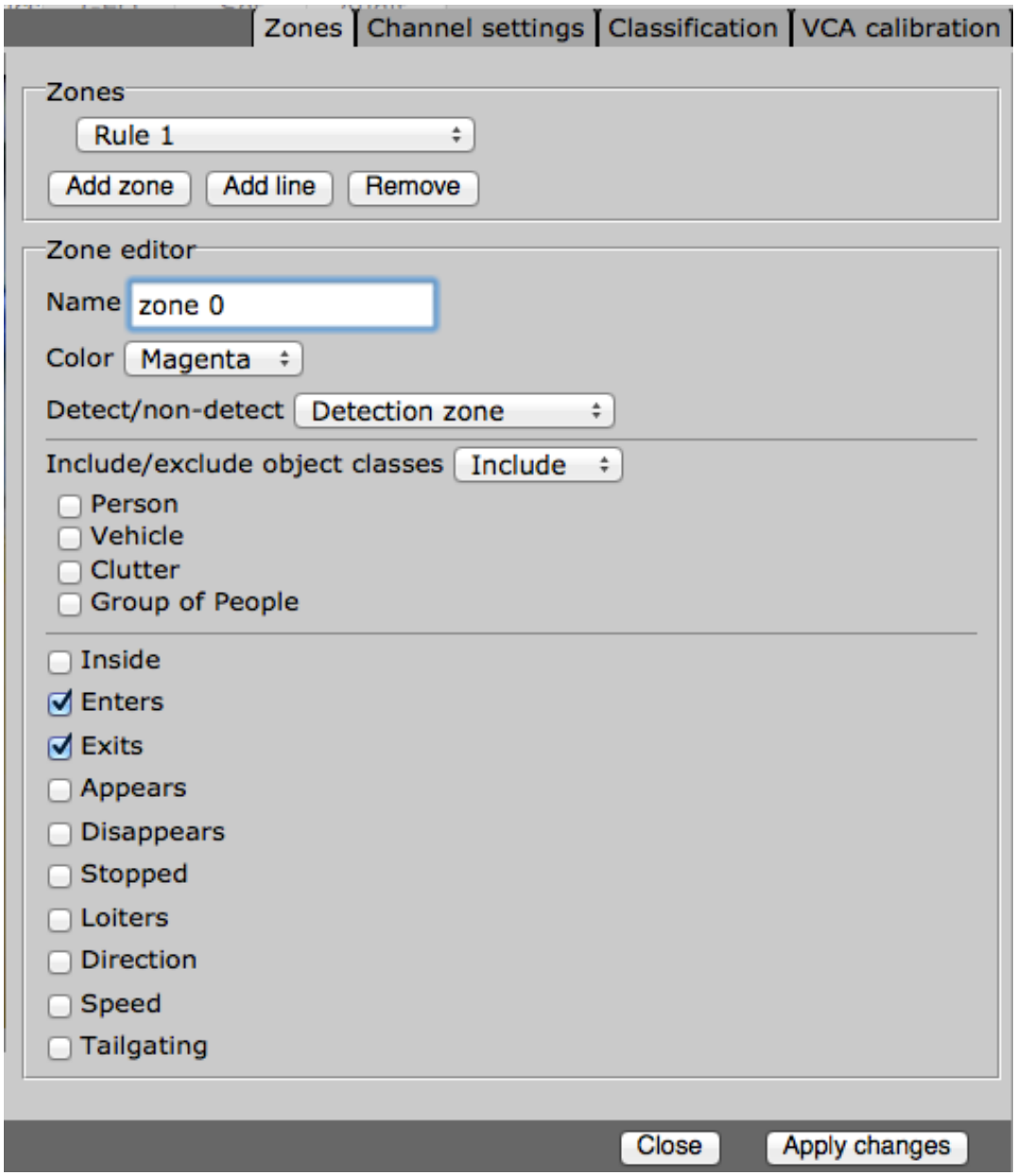


Figure A.2. VCA Analytics Zones

Table A.1. VCA Zone Configuration

Parameter	Description
Name	The name of the Rule. This name will be displayed in the event message when this rule is triggered.
Color	The configuration display color. This is useful when adding several rules, to be able to distinguish between them.
Detect/non-detect	Sets if the zone should be treated as a detection zone, or ignored as a non-detection zone.

Parameter	Description
Include/Exclude object classes	Set if detection should be run on selected object classifications, or NOT be run on selected classifications.
Object Classifications	These are classifications of objects. Additional classifications can be added, but defaults are: • Person • Vehicle • Clutter • Group of People For Classification to work accurately, all VCA settings must be properly configured.
Inside	Triggers an alert if the object is inside the zone.
Enters	Triggers an alert if the object enters the zone.
Exits	Triggers an alert if the object exits the zone.
Appears	Triggers an alert if the object appears in the zone (such as a zone placed over a door).
Disappears	Triggers an alert if the object disappears in the zone.
Stopped	Triggers an alert if an object stops in the zone. Additional Parameters: • Time - The number of seconds the object has stopped before triggering an alert. Maximum of 50 seconds.
Loiters	Triggers an alert if an object enters a zone but does not leave it. • Duration - The number of seconds that the object needs to be loitering before triggering an alert. Minimum of 20 seconds, maximum of 1 hour.
Direction	Triggers an alert if an object in the zone move in a certain direction. Additional Parameters: • Direction - The angles in degrees from "Up" on the image that the object needs to be moving for an alert to trigger. Value ranges from -180 to 180 degrees. • Acceptance Angle - The number of degrees off of from the set direction the target can be moving to still trigger an alarm. Value ranges from 0 to 360 degrees.

Parameter	Description
	When set, an arrow will be displayed on the zone indicating the direction an object needs to move to trigger (based on the "Direction" value). Two additional lines will be connected to the arrow, indicating the Acceptance Angle.
Speed	Triggers an alert if the object moves faster or slower than the set speeds. Additional Parameters: • Lower Bound - If the object is moving below this speed, an alert will be triggered. Values from 0 to 655 km/h. • Upper Bound - If the object is moving above this speed, an alert will be triggered. Value ranges from 0 to 655 km/h. This option relies heavily on accurate settings in the VCA Calibration tab, and other tabs.
Tailgating	Triggers an alert if one object follows another through the zone. Additional Parameters: • Threshold - The maximum number of seconds behind the first object that the second object must be to still trigger an alert. Value ranges from 0 seconds to 1 hour.

A.2.2. VCA - Adding and Editing Lines.

If you click the "Add Line", a line will be displayed in the video, and additional configuration options will be displayed on the right.

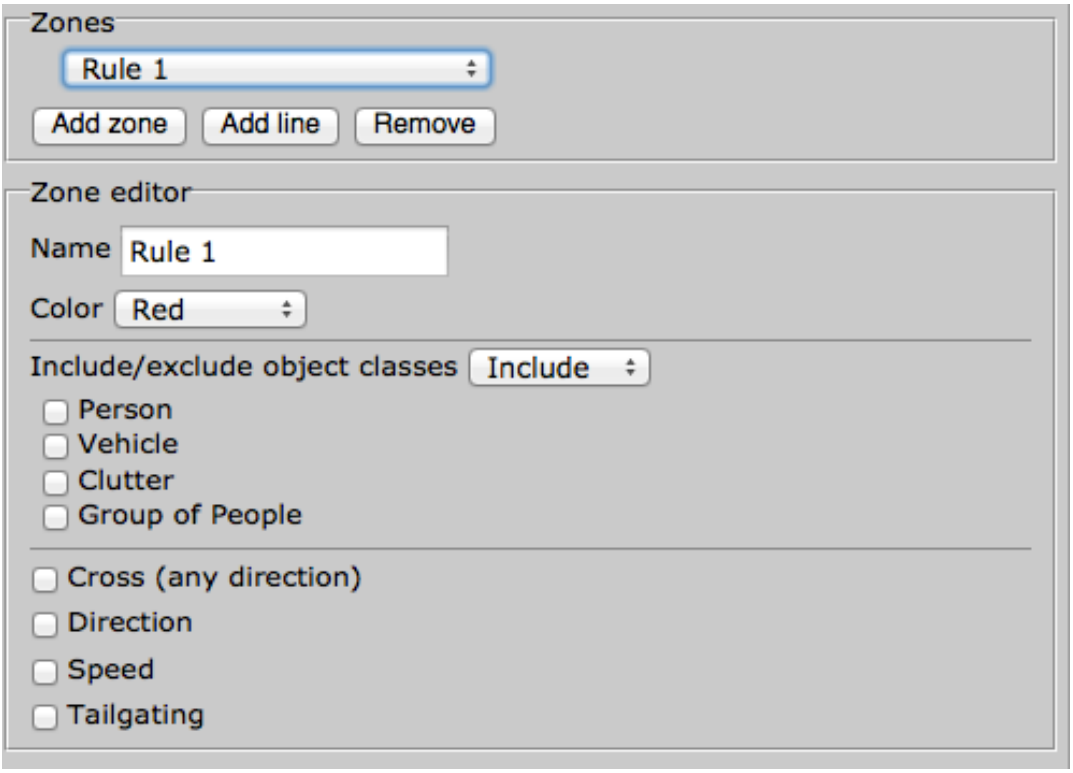


Figure A.3. VCA Analytics Lines

Table A.2. VCA Line Configuration

Parameter	Description
Name	The name of the Rule. This name will be displayed in the event message when this rule is triggered.
Color	The configuration display color. This is useful when adding several rules, to be able to distinguish between them.
Detect/non-detect	Sets if the zone should be treated as a detection zone, or ignored as a non-detection zone.
Include/Exclude object classes	Set if detection should be run on selected object classifications, or NOT be run on selected classifications.
Object Classifications	These are classifications of objects. Additional classifications can be added, but defaults are: • Person • Vehicle • Clutter • Group of People

Parameter	Description
	For Classification to work accurately, all VCA settings must be properly configured.
Cross (Any Direction)	Triggers an alert if an object crosses the tripwire.
Direction	Triggers an alert if an object crosses the tripwire in a certain direction. Additional Parameters: • Direction - The angles in degrees from "Up" on the image that the object needs to be moving for an alert to trigger. Value ranges from -180 to 180 degrees. • Acceptance Angle - The number of degrees off of from the set direction the target can be moving to still trigger an alarm. Value ranges from 0 to 360 degrees. When set, an arrow will be displayed on the zone indicating the direction an object needs to move to trigger (based on the "Direction" value). Two additional lines will be connected to the arrow, indicating the Acceptance Angle.
Speed	Triggers an alert if the object moves faster or slower than the set speeds. Additional Parameters: • Lower Bound - If the object is moving below this speed, an alert will be triggered. Values from 0 to 655 km/h. • Upper Bound - If the object is moving above this speed, an alert will be triggered. Value ranges from 0 to 655 km/h. This option relies heavily on accurate settings in the VCA Calibration tab, and other tabs.
Tailgating	Triggers an alert if one object follows another through the tripwire. Additional Parameters: • Threshold - The maximum number of seconds behind the first object the second object must be to still trigger an alert. Value ranges from 0 seconds to 1 hour.

A.2.3. VCA - Channel Settings

Channel settings tab is where settings describing how object detection is done (instead of what object detection to do) is set.

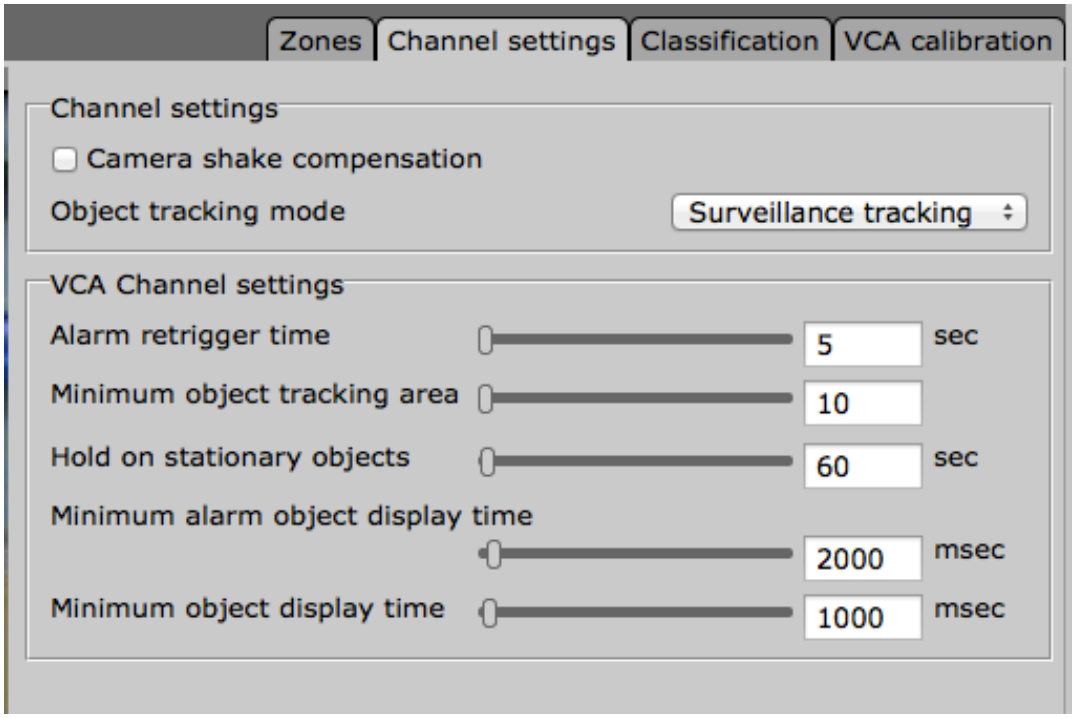


Figure A.4. VCA Analytics Channel Settings

Table A.3. VCA Channel Settings

Parameter	Description
Camera Shake Compensation	Sets if the analytics should attempt to compensate for camera shaking. This comes at two costs: 1. Reduced detection area. The shake compensation will remove up to 64 pixels per side of the video. This will potentially lower the total detection area significantly. 2. Increased CPU usage. Compensating for shake will take additional processing power to handle, so should be avoided if processing power looks tight.
Object Tracking Mode	Sets which object tracking mode to use. Currently, only Surveillance tracking is enabled.
Alarm Re-trigger Time	Sets the amount of time before the same alarm can be triggered by the same object an additional time.
Minimum Object Tracking Area	Sets the minimum size that an object can be and still be tracked, in square pixels.
Hold on stationary objects.	The amount of time to remember a stationary object, before it is considered part of the background. For example, it is unlikely that it is desirable to track a parked car for the entire day it is parked.
Minimum Alarm Object Display Time	The minimum time, in milliseconds, that an alarmed object will be displayed.

Parameter	Description
Minimum Object Display Time	The minimum time, in milliseconds, that an object will be displayed.

A.2.4. VCA - Classification

The Classification tab is to configure how objects are classified. It relies heavily on the VCA Calibration tab to have accurate settings.

At the top-left are listed already configured classifications. To add a new classification, click 'Add'. To remove a classification, select it and press 'Remove'. When an Object Class is selected, additional parameters are displayed on the bottom.

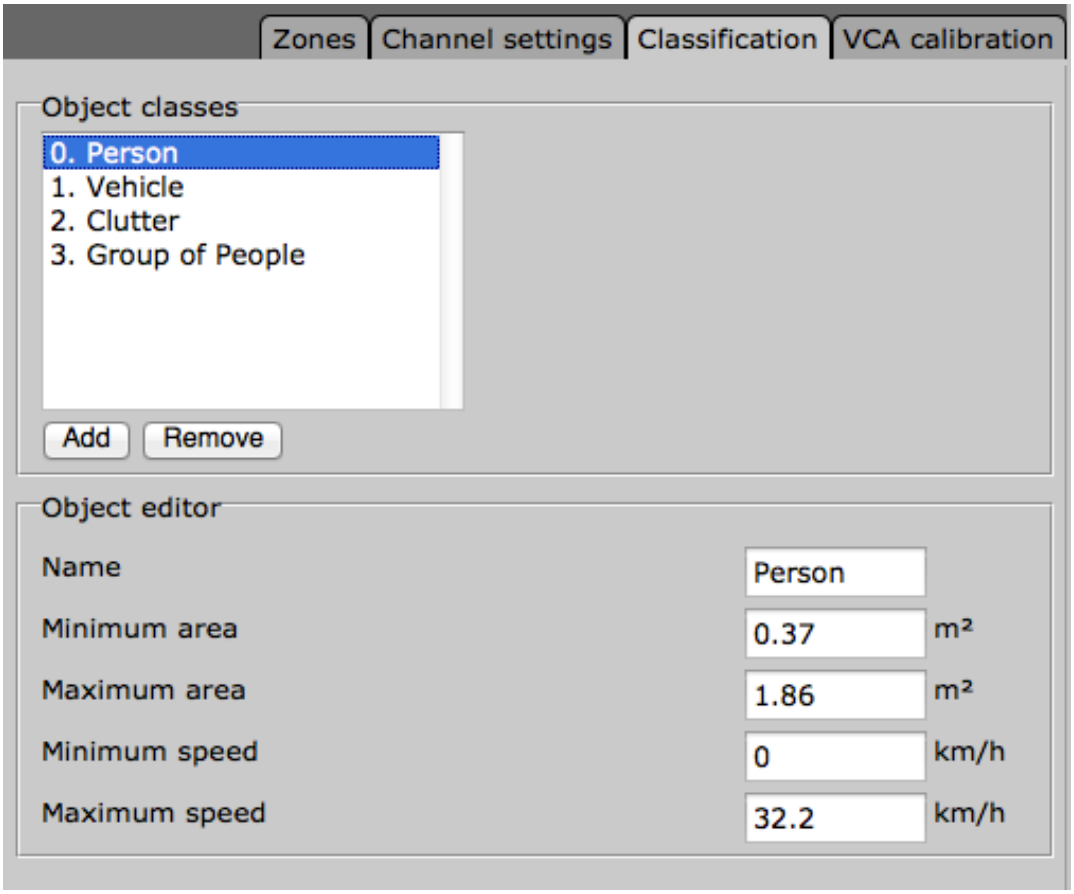


Figure A.5. VCA Analytics Classification

Table A.4. VCA Classification Settings

Parameter	Description
Name	The name of the classification, as it will appear in the list as well as the alert messages.
Minimum Area	The minimum area, in square meters, that the object must occupy to fall in to this classification category.
Maximum Area	The maximum area, in square meters, that the object must occupy to fall in to this classification category.

Parameter	Description
Minimum Speed	The minimum speed, in kilometers per hour, that the object must be moving to fall in to this classification category.
Maximum Speed	The maximum speed, in kilometers per hour, that the object must be moving to fall in to this classification category.

A.2.5. VCA - Calibration

The VCA Calibration tab is very important for many rules to properly function. It defines the cameras perspective, relative to the ground plane, allowing it to estimate object size and speed.

When on this tab, an overlay will be added to the video, showing a green grid representing the ground plane. When updating settings on this page, the overlay will reflect those changes.

If you double click on the ground plane, a virtual "meter stick" will be placed, shown in blue. This meter stick is meant to represent something two meters high, when properly calibrated.

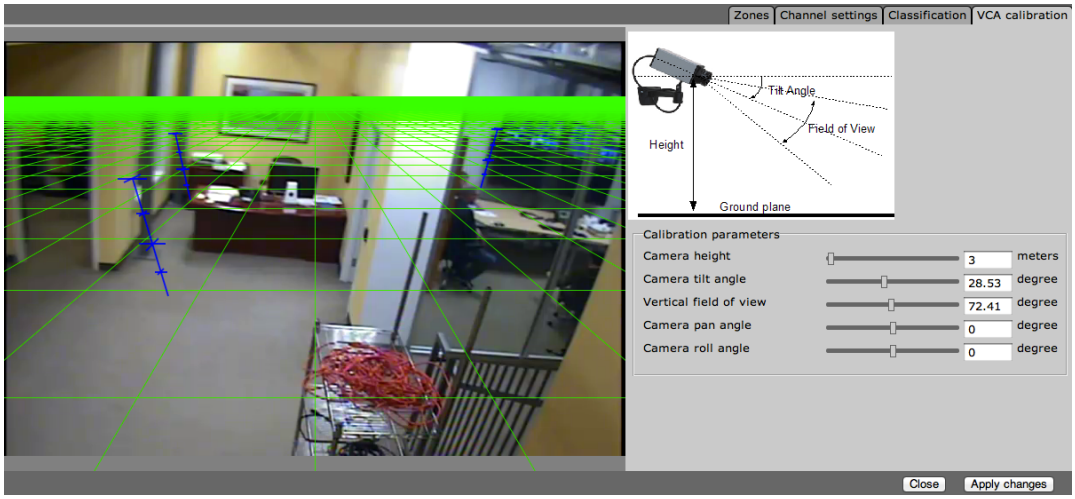


Figure A.6. VCA Analytics Calibration

Table A.5. VCA Calibration Settings

Parameter	Description
Camera Height	The height above the ground plane that the camera is at, in meters.
Camera Tilt Angle	The number of degrees the camera is looking below the horizon. Negative numbers means the camera is looking upwards.
Vertical Field of View	The angular distance the camera can see, from the top of the frame to the bottom.
Camera Pan Angle	The number of degrees the camera is paned, relative to the tilt plane.
Camera Roll Angle	The number of degrees the camera is rotated from horizontal.

A.3. OV Tracker Configuration

The OV behavior can be configured with Lines, Multilines, or Areas. There is an additional tab for View Settings. The following sub-sections will go in to more details about each.

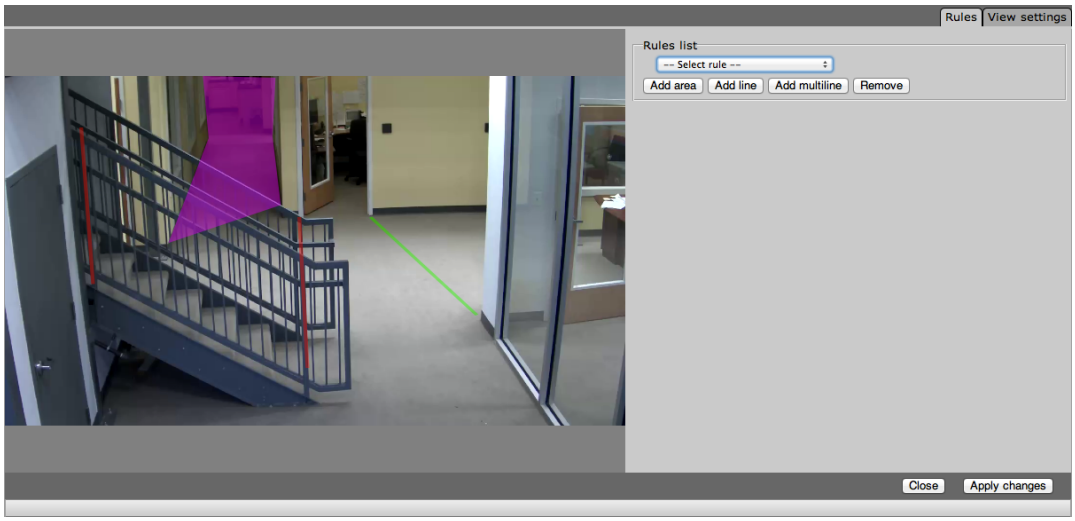


Figure A.7. OV Analytics Rules

A.3.1. OV - Adding and Editing Zones

If you click "Add Area", a small Area box will be displayed in the video, and additional configuration options will be displayed on the right.

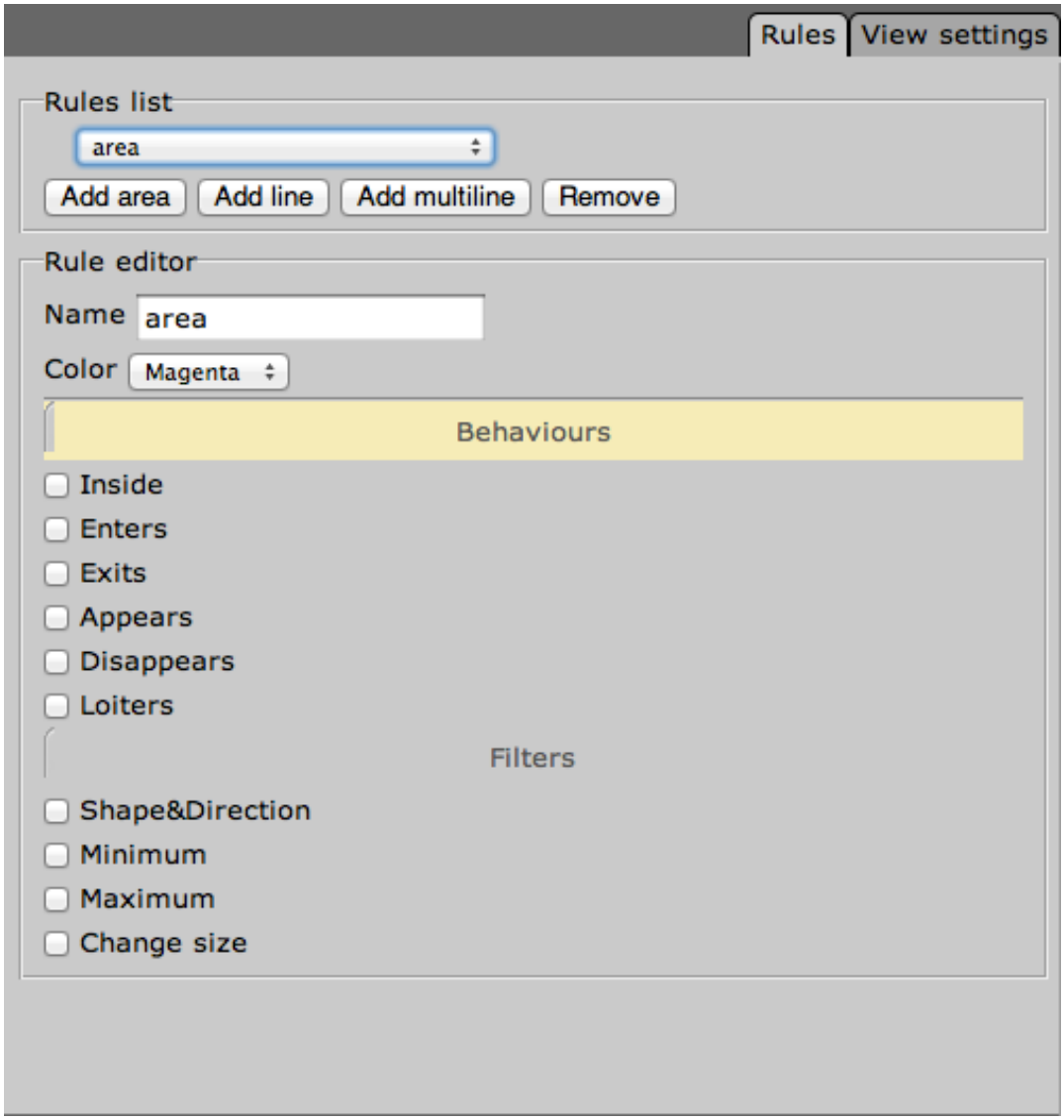


Figure A.8. OV Analytics Areas

Table A.6. OV Area Configuration

Parameter	Description
Name	The name of the Area. This name will be displayed in the event message when this area is triggered.
Color	The configuration display color. This is useful when adding several rules, to be able to distinguish between them.
Inside	Triggers an alert if the object is inside the area.
Enters	Triggers an alert if the object enters the area.
Exits	Triggers an alert if the object exits the area.
Appears	Triggers an alert if the object appears in the area (such as a zone placed over a door).

Parameter	Description
Disappears	Triggers an alert if the object disappears in the area.
Loiters	Triggers an alert if an object enters the area but does not leave it. • Duration - The number of seconds that the object needs to be loitering before triggering an alert. Minimum of 20 seconds, maximum of 1 hour.
Shape & Direction	Select to ignore objects that change shape or direction very rapidly. This option can be used to reduce false alerts caused by waves, shadows, etc.
Minimum	If an object is below a minimum size, it is ignored. Additional Parameters: • Near Width - The minimum width the object must be in the near ground, as a percentage of the screen, before it can trigger an alert. • Near Height - The minimum height the object must be the near ground, as a percentage of the screen, before it can trigger an alert. • Far Width - The minimum width the object must be far ground, as a percentage of the screen, before it can trigger an alert. • Far Height - The minimum height the object must be far ground, as a percentage of the screen, before it can trigger an alert.
Maximum	If an object is above a maximum size, it is ignored. Additional Parameters: • Near Width - The maximum width the object must be in the near ground, as a percentage of the screen, after which it is ignored. • Near Height - The maximum height the object must be the near ground, as a percentage of the screen, after which it is ignored. • Far Width - The maximum width the object must be far ground, as a percentage of the screen, after which it is ignored. • Far Height - The maximum height the object must be far ground, as a percentage of the screen, after which it is ignored.

Parameter	Description
Change Size	Sets the maximum change in size of an object can undergo before it is ignored. This change must occur rapidly to count. Additional Parameters: • Max change - The percent change, compared to the original object size. This value is used as a multiplier of total object area.

A.3.2. OV - Adding and Editing Lines.

If you click the "Add Line", a line will be displayed in the video, and additional configuration options will be displayed on the right.

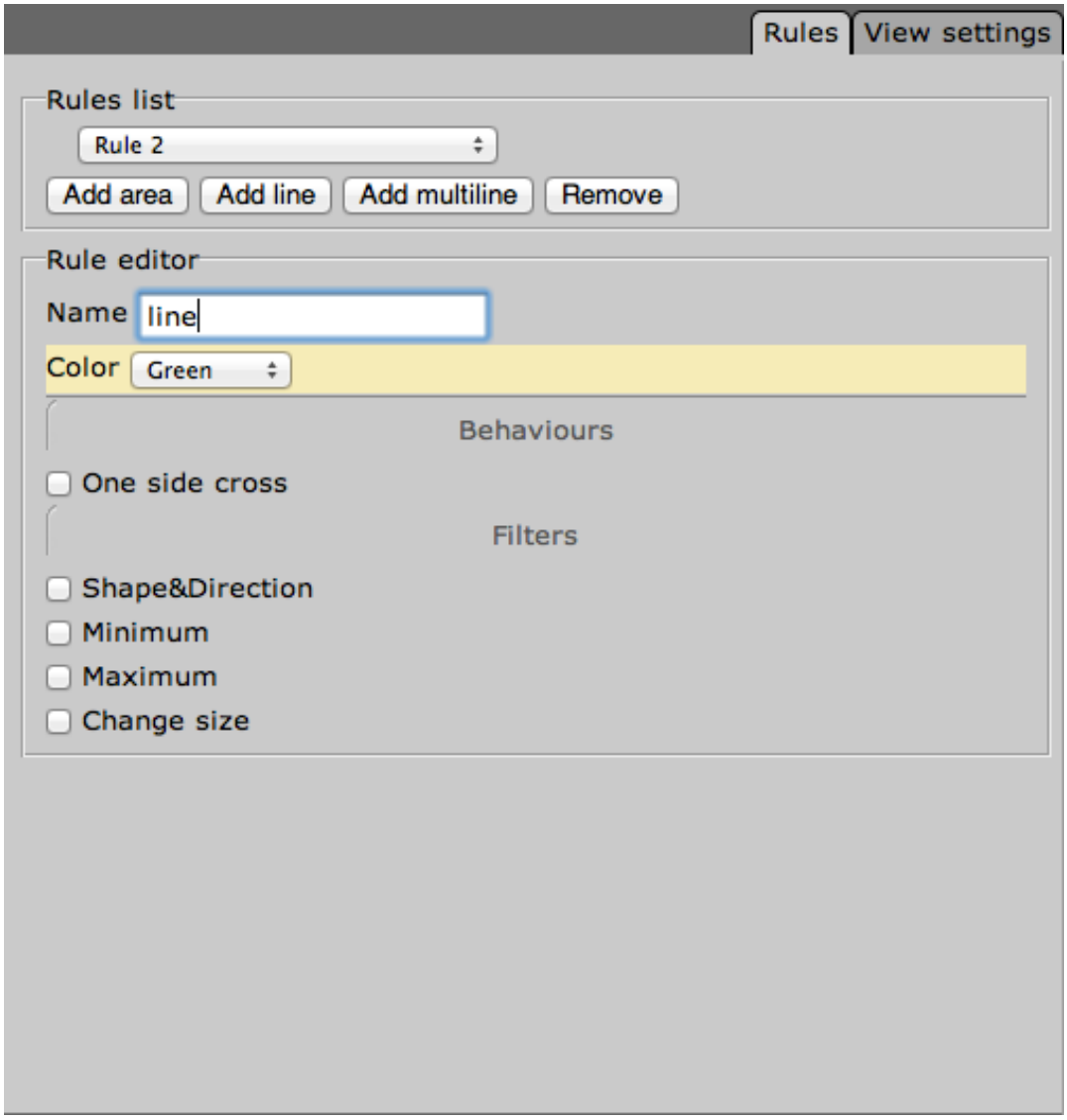


Figure A.9. OV Analytics Lines

Table A.7. OV Line Configuration

Parameter	Description
Name	The name of the Line. This name will be displayed in the event message when this rule is triggered.
Color	The configuration display color. This is useful when adding several rules, to be able to distinguish between them.
One Side Cross	Select to trigger alerts only if the object crosses the line in a certain direction. Additional Parameters: • Direction - Choose left-to-right or right-to-left. When chosen, an arrow will be added to the line indicating the direction the object must move to trigger the alert.
Shape & Direction	Select to ignore objects that change shape or direction very rapidly. This option can be used to reduce false alerts caused by waves, shadows, etc.
Minimum	If an object is below a minimum size, it is ignored. Additional Parameters: • Near Width - The minimum width the object must be in the near ground, as a percentage of the screen, before it can trigger an alert. • Near Height - The minimum height the object must be the near ground, as a percentage of the screen, before it can trigger an alert. • Far Width - The minimum width the object must be far ground, as a percentage of the screen, before it can trigger an alert. • Far Height - The minimum height the object must be far ground, as a percentage of the screen, before it can trigger an alert.
Maximum	If an object is above a maximum size, it is ignored. Additional Parameters: • Near Width - The maximum width the object must be in the near ground, as a percentage of the screen, after which it is ignored. • Near Height - The maximum height the object must be the near ground, as a percentage of the screen, after which it is ignored.

Parameter	Description
	• Far Width - The maximum width the object must be far ground, as a percentage of the screen, after which it is ignored. • Far Height - The maximum height the object must be far ground, as a percentage of the screen, after which it is ignored.
Change Size	Sets the maximum change in size an object can undergo before it is ignored. This change must occur rapidly to count. Additional Parameters: • Max change - The percent change, compared to the original object size. This value is used as a multiplier of total object area.

A.3.3. OV - Adding and Editing Multilines.

If you click the "Add Multiline", a line will be displayed in the video, and additional configuration options will be displayed on the right.

Multilines allow lower false-alerts than a single line. One object must cross both lines in order to trigger an alert.

Figure A.10. OV Analytics Multilines

Table A.8. OV Multiline Configuration

Parameter	Description
Name	The name of the Multiline. This name will be displayed in the event message when this rule is triggered.
Color	The configuration display color. This is useful when adding several rules, to be able to distinguish between them.
Ordered Crossing	Select to trigger alerts only if the object crosses both of the line in a certain order. Additional Parameters: • Order - Choose '1st then 2nd' or '2nd then 1st'. When chosen, an arrow will be added to both of the lines, indicating the direction the object must move to trigger the alert.

Parameter	Description
	• Duration - This is the maximum time a single object can take when crossing both lines. If the object takes longer than this period, an alarm will not be triggered.
Shape & Direction	Select to ignore objects that change shape or direction very rapidly. This option can be used to reduce false alerts caused by waves, shadows, etc.
Minimum	If an object is below a minimum size, it is ignored. Additional Parameters: • Near Width - The minimum width the object must be in the near ground, as a percentage of the screen, before it can trigger an alert. • Near Height - The minimum height the object must be the near ground, as a percentage of the screen, before it can trigger an alert. • Far Width - The minimum width the object must be far ground, as a percentage of the screen, before it can trigger an alert. • Far Height - The minimum height the object must be far ground, as a percentage of the screen, before it can trigger an alert.
Maximum	If an object is above a maximum size, it is ignored. Additional Parameters: • Near Width - The maximum width the object must be in the near ground, as a percentage of the screen, after which it is ignored. • Near Height - The maximum height the object must be the near ground, as a percentage of the screen, after which it is ignored. • Far Width - The maximum width the object must be far ground, as a percentage of the screen, after which it is ignored. • Far Height - The maximum height the object must be far ground, as a percentage of the screen, after which it is ignored.
Change Size	Sets the maximum change in size an object can undergo before it is ignored. This change must occur rapidly to count. Additional Parameters:

Parameter	Description
	• Max change - The percent change, compared to the original object size. This value is used as a multiplier of total object area.

A.3.4. OV - View Settings

Channel settings tab is where settings describing how object detection is done (instead of what object detection to do) is set.

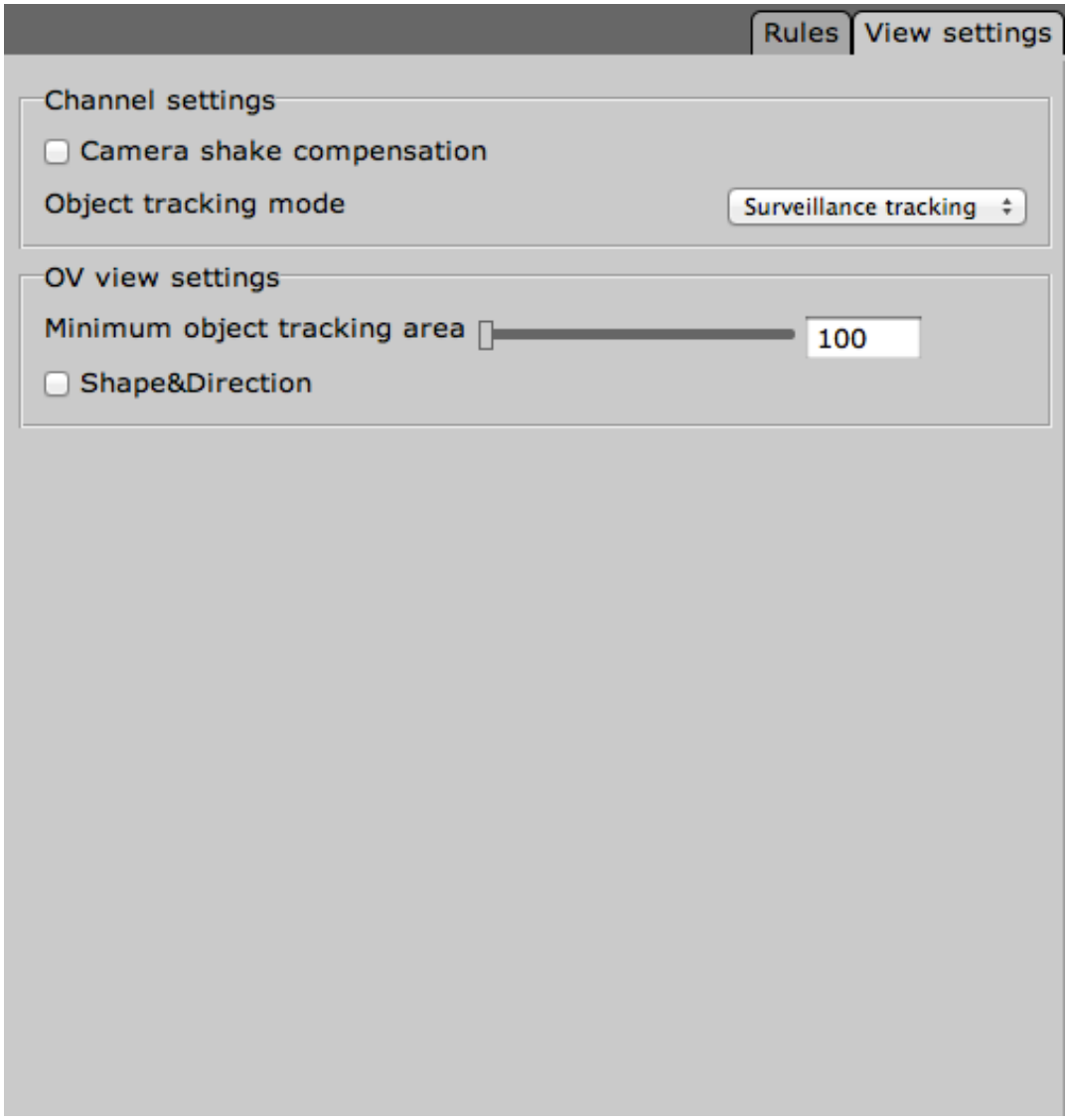


Figure A.11. OV Analytics View Settings

Table A.9. OV View Settings

Parameter	Description
Camera Shake Compensation	Sets if the analytics should attempt to compensate for camera shaking. This comes at two costs: 1. Reduced detection area. The shake compensation will remove up to 20 pixels per side of the video. This will potentially lower the total detection area significantly.

Parameter	Description
	2. Increased CPU usage. Compensating for shake will take additional processing power to handle, so should be avoided if processing power looks tight.
Object Tracking Mode	Sets which object tracking mode to use. Currently, only Surveillance tracking is enabled.
Minimum Object Tracking Area	Sets the minimum area an object must occupy to be tracked, in pixels. The default is the minimum, 100 pixels, or 10 pixels per side.
Shape & Direction	Select to ignore objects that change shape or direction very rapidly. This option can be used to reduce false alerts caused by waves, shadows, etc.

Appendix B. Video Codecs, Transmission Protocols and their Effective Usage

Digital video volumes are huge, so to make it commercially feasible and economical, video surveillance systems always rely upon some kind of video compression to reduce the size and effect on transmission lines and storage systems.

The surveillance industry took multiple approaches to accomplish this, but in the most common scenario they are based on either closed vendor specifications or open industry standards.

Stratus is based upon RTSP (Real-Time-Streaming-Protocol) an open industry standard for the transmission protocol and most prevalent standard MJPEG/MPEG-2/MPEG-4/H.264 codecs in use for video surveillance industry today.

You can easily find a tremendous amount of information about particular codec's advantages and drawbacks on the Internet, but here we will mostly concentrate on practical aspects of selecting one or another codec.

- Motion-JPEG (MJPEG) codec
  - The simplest of all, as every frame is a fully-independent JPEG image
  - The first standard codec in the Video Surveillance industry
  - The smallest latency among all other codecs in this group, as each frame is encoded individually and does not need any delay to get streamed out
  - The easiest to integrate
  - The quality is the best in the group
  - The bandwidth and storage space consumption is the largest in the group
  - Quality, bandwidth and storage utilization in general do not depend upon motion on the scene and are relatively constant
  - It is the fastest time to open stream and to reposition in the stream during playback
- MPEG-4 codec
  - This codec was introduced much later to compare to MJPEG, and this stream is a complex sequence of independent "key-frames" (I-frame) and "differential frames" (P-frames), which requires you to wait until next I-frame before stream may be visualize
  - Since P-frames do not need to repaint entire picture, this type of old stream is much more compact for relatively static scenes (relatively small amount of motion involved)
  - In general, storage and bandwidth utilization are significantly lower compared to MJPEG
  - MPEG-4 has a catch: it is compact when a scene is relatively static, but it will sharply increase bandwidth/storage utilization when a scene becomes very dynamic. Most manufacturers allow the limiting of these bursts, but at the price of decreased quality or decreased frame rate, so if it is not carefully configured, the video can become degraded to an unusable state.

  - MPEG-4 always has an additional latency present at the start of the visualization of the MPEG-4 stream, which is due to the skipping of frames next to the I-frame, which may last up to several seconds
  - Stream reposition and individual frames extraction obeys the same laws: it is possible with mandatory reposition to I-frame only, which may take additional time
- h.264 codec
  - This is the newest of all, and it is an evolution of MPEG-4 with all its advantages magnified and its disadvantages mostly preserved
  - H.264 is even more compact and quality is more consistent and better controlled
  - If you have a choice of H.264 or MPEG-4 for the new installation, there is no reason to use MPEG-4
- MPEG-2 codec
  - It may look like a step backward, but the security industry adopted MPEG-2 for number of unique characteristics
  - MPEG-2 was originally designed and optimized for DVD and thus is concerned primarily about the video quality
  - The advantages and drawbacks are similar to MPEG-4 and H.264, but the focus is shifted to better video quality at expense of additional bandwidth and latency
  - MPEG-2's relevant hardware is mostly a niche market nowadays

Given listed codecs' specifics, we recommend:

- Skipping MPEG-4 in favor of H.264 when possible
- Use MJPEG for the situations when real-time performance is mostly required and when bandwidth / storage is not of concern
- Use H.264 (or MPEG-4) when you are mostly concerned about long-term storage, and a few tenths of a second of extra latencies may be sacrificed

Appendix C. Detailed Steps

C.1. Stratus software Installation in details

C.1.1. Prepare OS (Linux only)

Assumptions:

- You should have a Red Hat Enterprise Linux 5 update 7 installation media (download from *http://www.redhat.com/apps/download/*) burned to a DVD
- You have downloaded the KickStart file from videoNEXT web portal (go to*portal login*[1] and then Downloads section).
- You should have USB drive with videoNEXT KickStart (please unpack ks-stratus-3.3.X.zip file into root directory of your USB stick)
- You should decide on the network configuration to be used (IP address, name, network mask, router, DNS etc...). Please contact you Network Admin for specifics.

Installation Steps:

1. Insert DVD with Red Hat Enterprise Linux 5 into your server's DVD drive and start an RHEL installation. You may use either an internal DVD drive or a USB-attached external DVD drive. Check the BIOS boot order and make sure your DVD drive is the fist bootable device. Do not insert USB-stick into the server yet.
2. Once the Installation starts you will get the boot screen. Type **`linux ks=hd:sda:/none`**. (At this point we set dummy installation kick-start file location since we do not know what name our USB-stick will get.)

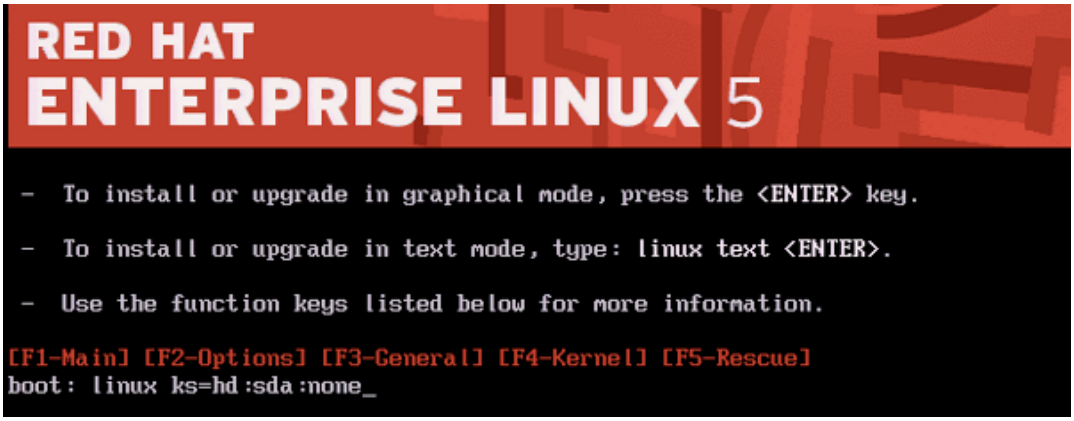

RED HAT
ENTERPRISE LINUX 5
- To install or upgrade in graphical mode, press the <ENTER> key.
- To install or upgrade in text mode, type: linux text <ENTER>.
- Use the function keys listed below for more information.
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: linux ks=hd:sda:none_

Figure C.1. The 'Boot: ' Screen

3. The kick-start scenario will be initialized and in less than a minute you will get the screen requesting kickstart-file path clarification:

[1] http://vtiger.videonext.com/portal

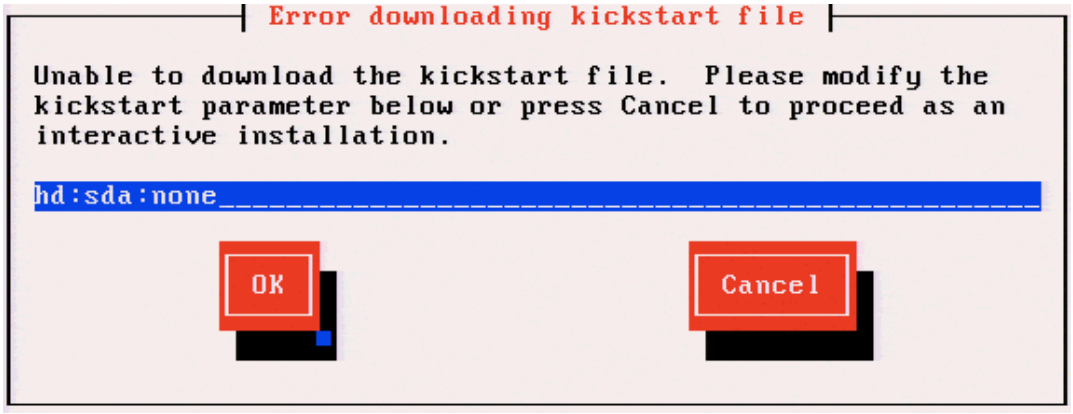

Error downloading kickstart file
Unable to download the kickstart file. Please modify the kickstart parameter below or press Cancel to proceed as an interactive installation.
hd:sda:none
OK
Cancel

Figure C.2. Provide location of kickstart

4. Insert your USB-stick into the server. Press <ALT+F4> to switch the console to the installation log. You need to find the actual USB-drive name on the screen. The name depends upon the server configuration and may be different. In our example it is **sdh1**:

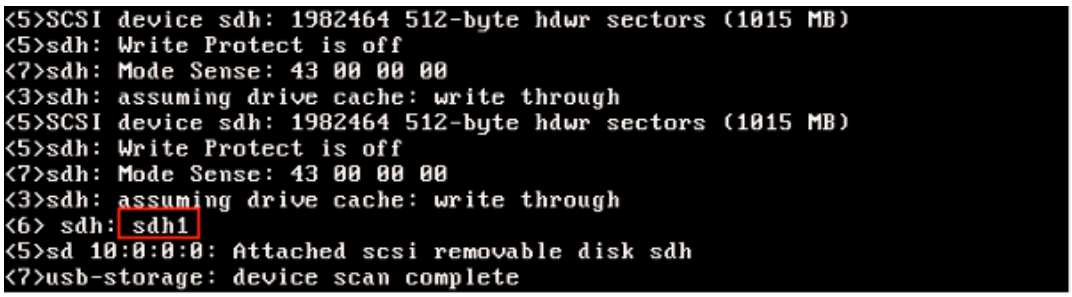

<5>SCSI device sdh: 1982464 512-byte hdwr sectors (1015 MB)
<5>sdh: Write Protect is off
<7>sdh: Mode Sense: 43 00 00 00
<3>sdh: assuming drive cache: write through
<5>SCSI device sdh: 1982464 512-byte hdwr sectors (1015 MB)
<5>sdh: Write Protect is off
<7>sdh: Mode Sense: 43 00 00 00
<3>sdh: assuming drive cache: write through
<6> sdh: sdh1
<5>sd 10:0:0:0: Attached scsi removable disk sdh
<7>usb-storage: device scan complete

Figure C.3. Find USB device

5. Press <ALT+F1> to switch back into the installation dialog and type the actual kick-start path (substituting the disk name found in previous step). The final kickstart name in our example is: **`hd:sdh1:stratus.cfg`**

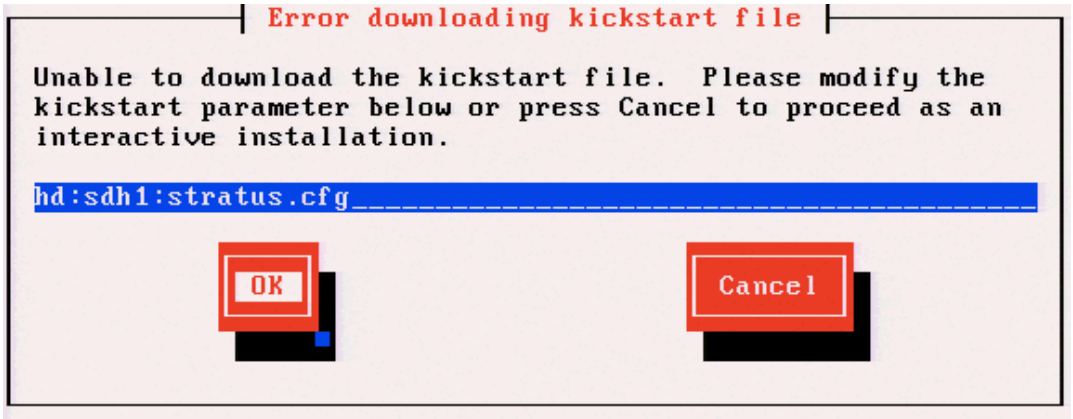

Error downloading kickstart file
Unable to download the kickstart file. Please modify the kickstart parameter below or press Cancel to proceed as an interactive installation.
hd:sdh1:stratus.cfg
OK
Cancel

Figure C.4. Kickstart Path

6. The kickstart will start the network configuration dialog. You will need to configure at least one network interface at this time.

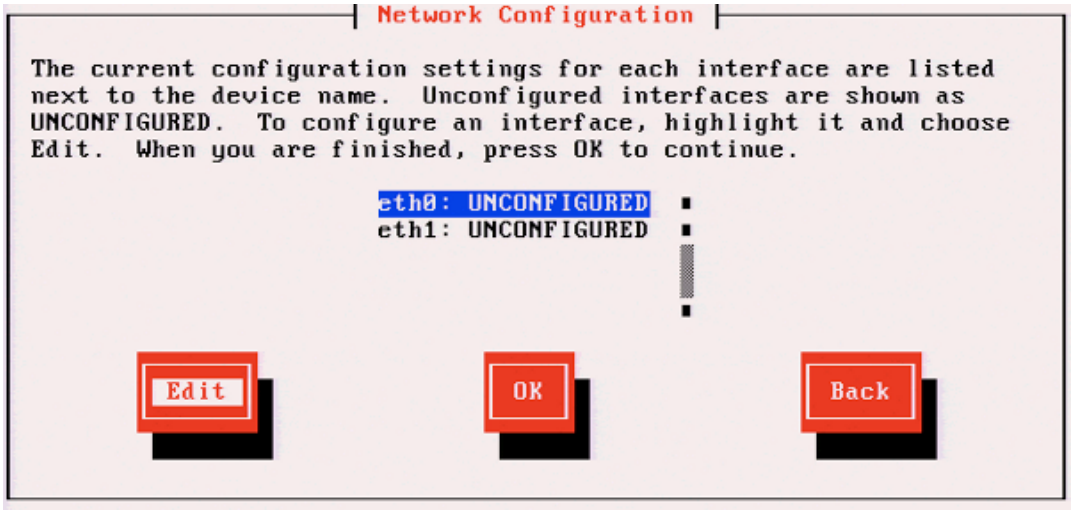

Network Configuration
The current configuration settings for each interface are listed next to the device name. Unconfigured interfaces are shown as UNCONFIGURED. To configure an interface, highlight it and choose Edit. When you are finished, press OK to continue.
eth0: UNCONFIGURED
eth1: UNCONFIGURED
Edit
OK
Back

Figure C.5. Network Configuration 1

7. You will need to chose either the DHCP or Static Network configuration. The following example will be based on a static network address choice:

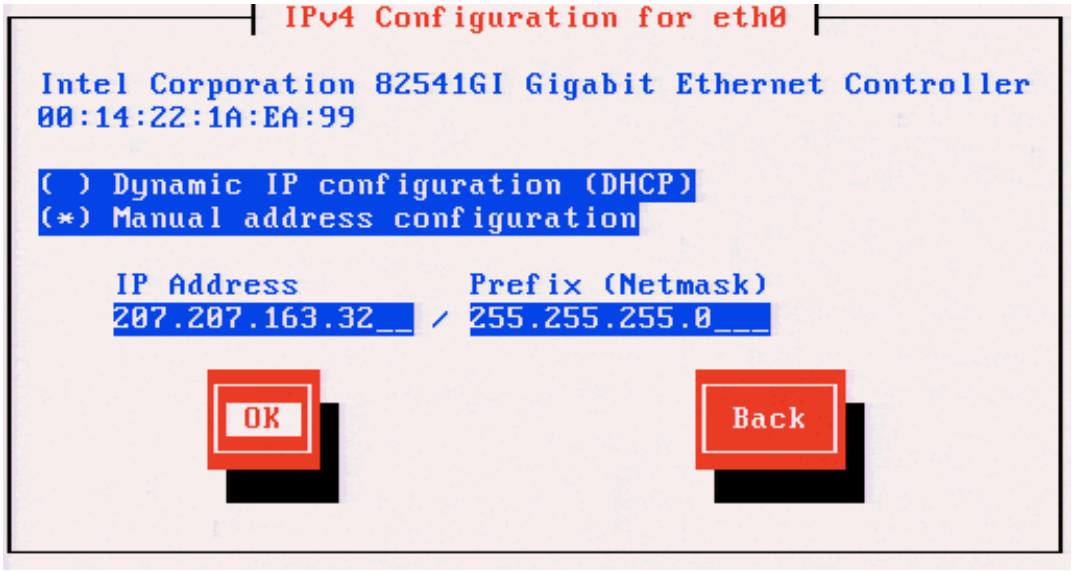


Figure C.6. Network Configuration 2

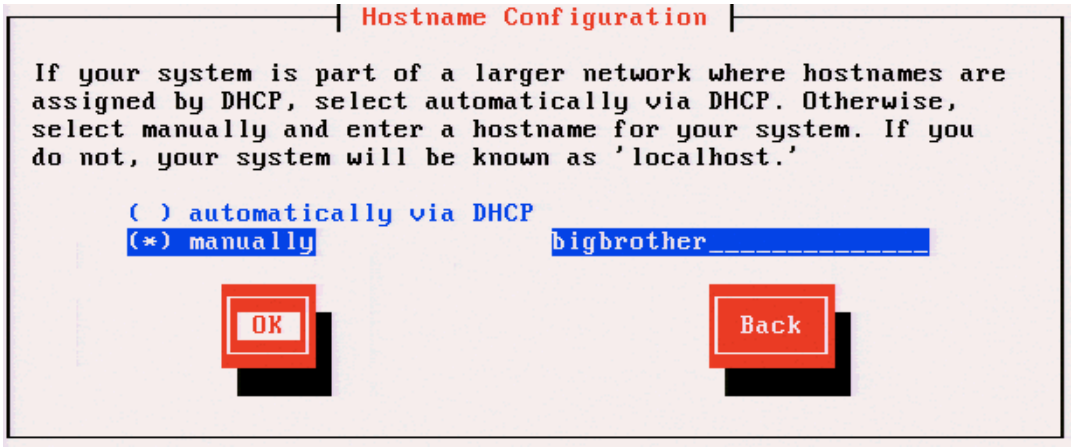

Hostname Configuration
If your system is part of a larger network where hostnames are assigned by DHCP, select automatically via DHCP. Otherwise, select manually and enter a hostname for your system. If you do not, your system will be known as 'localhost.'
( ) automatically via DHCP
(*) manually
bigbrother
OK
Back

Figure C.7. Network Configuration 3

8. Assign the name for the server, especially if you do not have a DHCP server to automatically do that for you.

9. Next the kick-start will begin installing all required packages. This may take a few minutes. You will see screens like this:

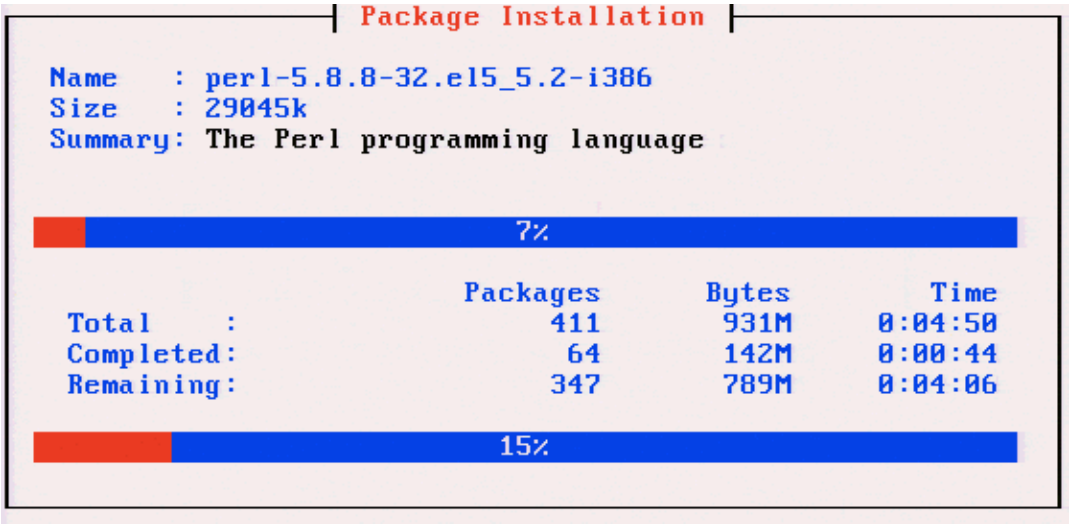


Figure C.8. Network Configuration 4

10. When the installation is complete, the server will eject the DVD and restart itself.

Activation:

1. Login with as "**sos**" user (password **s.o.s.**). You will be prompted to change the password.

   Switch to the root account with the command **su -**. The default password will be **123456**. You will be prompted to change the password.

   Run the activation script with the command **/opt/sarch/bin/activate**.

   The following activation dialog will be presented:

```
Define an activation scenario by combining the TYPE with multiple options
---------------------- TYPE --------------------------
 M - Master      Dedicated master or master only system
 N - Node        Install an additional node for a system
 E - Evaluation  Master only system with small storage on system drive
---------------------- options -----------------------
 m - MUMS           (Mass Update Management System)
 s - SOS Account
 f - Format Storage (Find potential storage drives and format them)
 t - Setup NTP
 c - Custom scripts (run scripts from USB drive prior and after activation)
------------------------------------------------------
Example: Mf - installs Master System and format the storage
? Ms
```

2. You must choose only one option from the TYPE category, and you can choose none or any of the second options

   For most installations you will want to choose '**Ms**' at the least.

Warning

If you choose the '**f**' option, the system will attempt to format any attached storage it sees (such as the USB drive with the Kickstart on it, if it is still present). Do not choose this option unless you know all attached storage is safe to be formatted.

3. The activation process takes a few minutes but may take substantially longer if the optional step “Format Storage” is chosen.

4. After activation is completed use your workstation browser (Internet Explorer 8, FireFox, or Chrome are recommended) for connecting to the server and configuring cameras.

   The predefined system administrator user: **admin**, password: **topse**.

C.1.2. CentOS Linux

An alternate means of installing the Stratus software for Linux is to use the CentOS version. This version has some advantages over the Red Hat version:

- It is free to download.
- The installation DVD contains the entire software, no need to use a USB drive.
- The installation procedure is much easier.
- The installation DVD is a very smaller download (under 1GB).

The CentOS version is functionally identical to the Red Hat version. The only downside is that you have no support for any problems that may occur with the Operating System. If this is acceptable for your installation, we recommend that you use the CentOS version instead.

Assumptions:

- You should have a CentOS-5.7-stratus-3.3-X.dvd.iso installation media (download from the downloads section at *http://vtiger.videonext.com/portal/*[2]) burned to a DVD
- You should decide on the network configuration to be used (IP address, name, network mask, router, DNS etc...). Please contact you Network Admin for specifics.

Installation Steps:

1. Insert the DVD with Stratus and CentOS 5.7 into your server's DVD drive and start an CentOS installation. You may use either an internal DVD drive or a USB-attached external DVD drive. Check the BIOS boot order and make sure your DVD drive is the fist bootable device.

2. Once the Installation starts you will get the boot screen. Type **stratus** and press enter. This tells the system to install everything needed for the Stratus software, and the Stratus software itself.

[2] vtiger.videonext.com/portal

3. The installation will start the network configuration dialog. You will need to configure at least one network interface at this time.

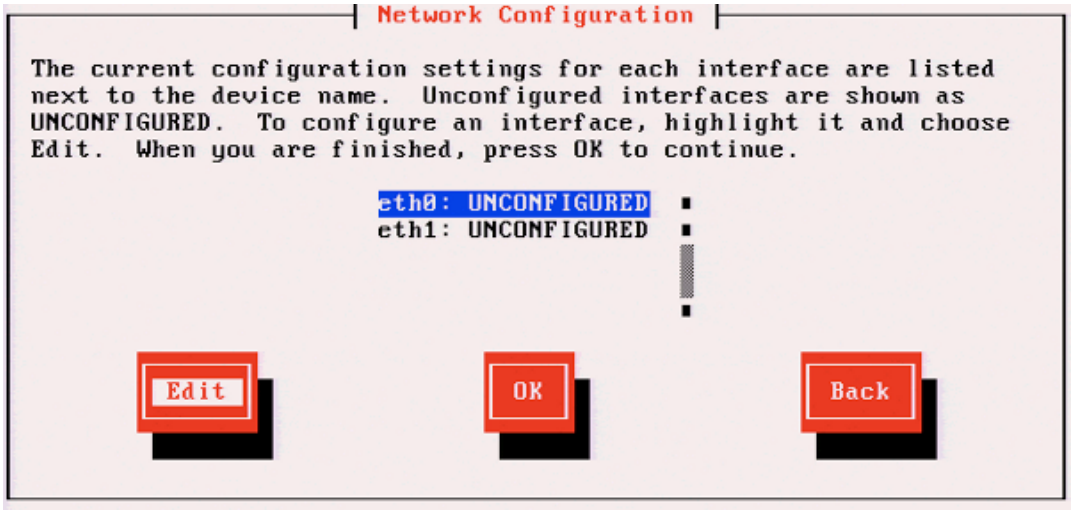

Network Configuration
The current configuration settings for each interface are listed next to the device name. Unconfigured interfaces are shown as UNCONFIGURED. To configure an interface, highlight it and choose Edit. When you are finished, press OK to continue.
eth0: UNCONFIGURED
eth1: UNCONFIGURED
Edit
OK
Back

Figure C.9. Network Configuration 1

4. You will need to chose either the DHCP or Static Network configuration. The following example will be based on a static network address choice:

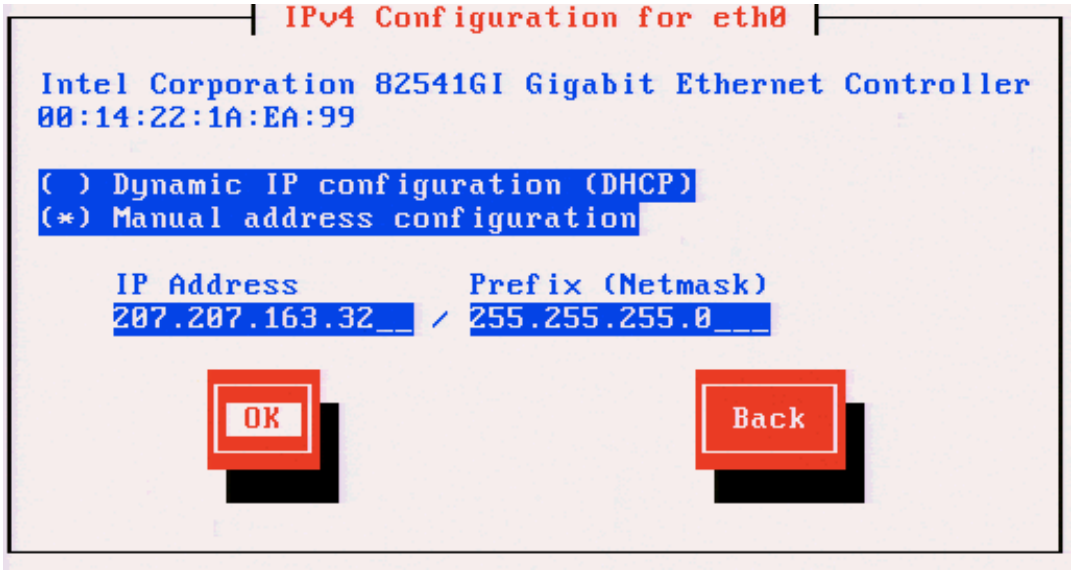


Figure C.10. Network Configuration 2

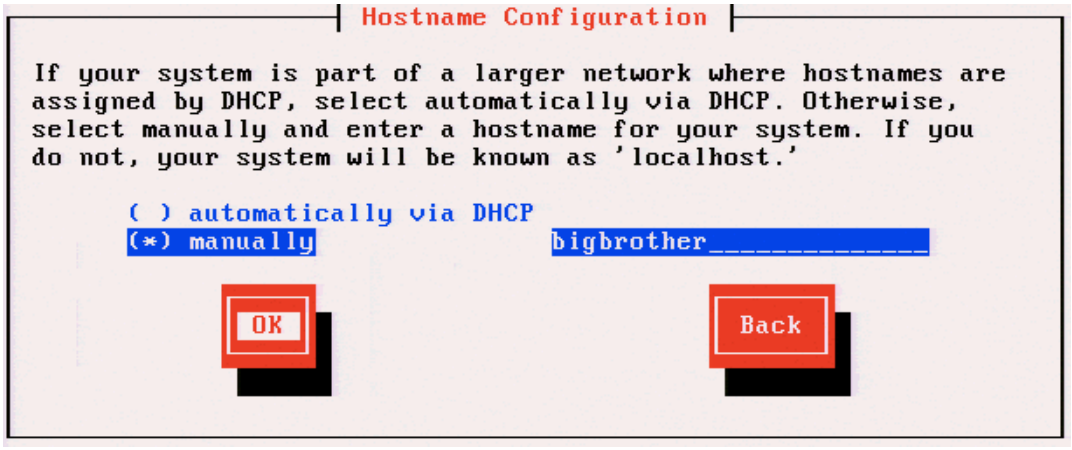

Hostname Configuration
If your system is part of a larger network where hostnames are assigned by DHCP, select automatically via DHCP. Otherwise, select manually and enter a hostname for your system. If you do not, your system will be known as 'localhost.'
( ) automatically via DHCP
(*) manually
bigbrother
OK
Back

Figure C.11. Network Configuration 3

5. Assign the name for the server, especially if you do not have a DHCP server to automatically do that for you.

6. Next the installation will begin installing all required packages. This may take a few minutes. You will see screens like this:

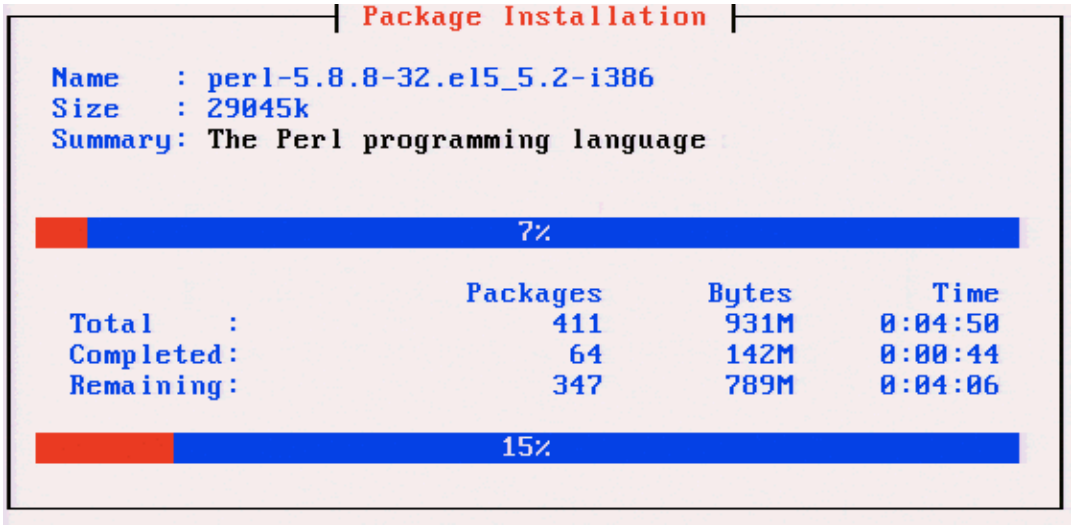


Figure C.12. Network Configuration 4

7. When the installation is complete, the server will eject the DVD and restart itself.

Activation:

1. Login with as "**sos**" user (password **s.o.s.**). You will be prompted to change the password.

   Switch to the root account with the command **su -**. The default password will be **123456**. You will be prompted to change the password.

   Run the activation script with the command **/opt/sarch/bin/activate**.

   The following activation dialog will be presented:

```
Define an activation scenario by combining the TYPE with multiple options
---------------------- TYPE --------------------------
 M - Master      Dedicated master or master only system
```

```
 N - Node        Install an additional node for a system
 E - Evaluation  Master only system with small storage on system drive
---------------------- options -------------------------
 m - MUMS           (Mass Update Management System)
 s - SOS Account
 f - Format Storage (Find potential storage drives and format them)
 t - Setup NTP
 c - Custom scripts (run scripts from USB drive prior and after activation)
-------------------------------------------------------
Example: Mf - installs Master System with sos and format the storage
? Ms
```

2. For most installation you will want to choose '**Ms**' at the least.

Warning

If you choose the '**f**' option, the system will attempt to format any attached storage it sees (such as the USB drive with the Kickstart on it, if it is still present). Do not choose this option unless you know all attached storage is safe to be formatted.

3. The activation process takes a few minutes but may work substantially longer if the optional step “Format Storage” is chosen.

4. After activation is completed use your workstation browser (Internet Explorer 8 or Chrome are recommended) for connection to the server and configuring cameras.

   The predefined system administrator user: **admin**, password: **topse**.

C.2. Upgrade from Stratus 2.7.1

This Appendix contains a detailed description of the process which for the Stratus system upgrade from version 2.7.1 to 3.3.

At this time, there is no upgrade path from 2.7.1 to 3.3.

C.3. Software Upgrade

When performing a software upgrade, Stratus will be unavailable and not recording. Some upgrades will require the system to be restarted, check the release notes that come with new software versions. In most cases, all nodes will need to be upgraded to the newest software version at the same time. Plan downtime accordingly.

C.3.1. Software Upgrade Through SOS Account

If you have the "S.O.S." account enabled, performing software updates is easy. (For more general information on using the "S.O.S." account, see *Section C.4, “Using “S.O.S.” Account for system administration/recovery (Linux only)”*)

When logged in to the "S.O.S." menu, perform the following steps to upgrade the software:

1. Choose option **7** to start the update process.

2. The system will pause and ask you to provide the new software version at this time. There are two methods of presenting the software to Stratus:

a. Place the software on a USB and connect the USB to the server. The upgrade process will automatically check attached USB devices for newer software.

b. Place the software in the */mnt* folder. This could be where you copy the software to, if you are remotely connected, or this could be the mount point of some non-USB drive (like a CD/DVD).

3. Once the software is on the system, press **ENTER** to continue. If the system is unable to identify the software where you placed it, it will display "Nothing was found" and return.

C.3.2. Software Upgrade

The software upgrade procedure in 3.3 is very simple. In this version we have done away with the concept of "Service Packs", and instead you just install a new "rpm" package containing the newest code.

Before getting started, you will need to prepare the following:

1. Download the newest software version from the videoNEXT portal.
2. Take note of the new software's name. Below we will use the example name "va-stratus-3.3.2-1.el5.rpm" (meaning version 3.3, patch 2, build 1), but this will likely not be the exact name that you download.
3. Identify the path to the software. The path might be the current directory, the path to a USB-drive, or even an FTP URL. In the examples, I will be using a path as if the software is at the path "/home/sos/", the home directory of the 'sos'. See *Section C.3.3, "Remote Software Upgrade"* for how to push the software through "scp", and steps to copy from a USB-drive
4. Remove the old version of Stratus

```
# rpm -e va-stratus
```

5. Install the new version you copied over.

```
#rpm -i va-stratus-3.3.2-1.el5.rpm
```

6. Once the installation is complete, you will need to run the activation script.

```
# /opt/sarch/bin/activate
```

You will be asked if you want to make a "C - Clean" install, or "U - Upgrade". A clean install will wipe all configuration and license. An upgrade will leave configuration and licensing intact.

C.3.3. Remote Software Upgrade

The service pack can also be installed remotely, but doing so requires more complicated steps.

In order to perform a remote upgrade you will need an SSH and SCP client. This should come standard on any Linux or Mac OS platform. For Windows users, a free utility is PuTTY, available from `www.putty.org`, where you will want to get putty.exe and pscp.exe.

1. Acquire the service pack as described in the section above.
2. You will need to push the service pack to the server using SCP. In the following example the service pack is in the home directory:

```
$ scp ~/va-stratus-3.3.2-1.el5.rpm sos@<Stratus_ip>:~/
```

You will need to replace '<stratus_ip>' with the address of your Stratus server. This will then prompt for the 'sos' password and place the file in the 'sos' user's home directory.

3. Now remotely login to the server with SSH:

```
$ ssh sos@<Stratus_ip>
```

4. Once logged in, you will need to switch to root,

```
$ su -
```

5. Change directories to 'sos' home where you copied the service pack.

```
# cd ~sos
```

6. Remove the old version of Stratus

```
# rpm -e va-stratus
```

7. Install the new version you copied over.

```
#rpm -i va-stratus-3.3.2-1.el5.rpm
```

8. Once the installation is complete, you will need to run the activation script.

```
# /opt/sarch/bin/activate
```

You will be asked if you want to make a "C - Clean" install, or "U - Upgrade". A clean install will wipe all configuration and license. An upgrade will leave configuration and licensing intact.

C.4. Using “S.O.S.” Account for system administration/ recovery (Linux only)

When the Stratus software is installed, it creates a special “S.O.S.” account on every Stratus node (server), which is used specifically for system configuration, patches, and recovery operations. It is accessible from the system console only or ssh, and has “s.o.s.” as the default password.

```
================================ Network ====================================
bond0: 207.207.160.10/255.255.255.0
nameserver 207.207.160.1        : OK
nameserver 207.207.160.2        : OK
-------------------------------- NTP Server ---------------------------------
     remote           refid      st t when poll reach   delay   offset  jitter
 127.127.1.0     .LOCL.          10 l   49   64  377    0.000    0.000   0.001
*207.207.160.1   129.6.15.28      2 u  345 1024  377    0.129   26.975   1.543
---------------------------- System ID/version -----------------------------
33STR131853856901 / va-stratus-3.3.1-6.el5-p0
------------------------------- Application ----------------------------------
Application is UP and RUNNING
Status:ALERT
Camera vChain 3.2.0 [210] is BROKEN
---------------------------- NODE / DOMAIN   -------------------------------
Master IP: 207.207.160.10
Server is MASTER
================================================================================
                    Select an option:
1. Show status                          |   6. Reset application admin password
2. Network/DNS configuration            |   7. System update
3. Change MASTER IP                     |   8. Setup NTP Server
4. Restart application services         |   9. Collect Support Files
5. Restart server                       |  99. EXIT
? 
```

Figure C.13. The 'sos' interface

The “S.O.S.” account displays an overview of the system status. It will show the IP and netmast, configured nameservers and if they are reachable, current NTP status, the license and software version, the system state and any status messages, the Master's IP address, and the current computers running state (node or master).

Various options also allow the settings to be changed. The options are:

1. Show status - shows the system status (as above).
2. Network/DNS configuration - change the network information, or DNS information.
3. Change MASTER IP - This option will change the IP address the server is looking to as the Master. On Master nodes, you will only be able to set "Master IP" to one of the network interaces present on the system. If chosen on a Node, the Node will attempt to varify that the IP belongs to a Master.
4. Restart application serveices - This will restart all services related to the running of Stratus. This includes Stratus, the database, and the web interface.
5. Restart server - This restarts the entire server. it is equivalent to running the "Reboot" command.
6. Reset application admin password - If admin log in credentials are lost or otherwise unavailable, this allows the credentials to be reset.
7. System Update - see *Section C.3.1, “Software Upgrade Through SOS Account”*.
8. Setup NTP server (only available o the Master) - This option configures where the Master should look for an NTP server. Nodes always look to the master as their NTP source.

9. Collect Support Files - This will collect various logs and system statistice and compress them in to one file. Uploading this file when requesting support can greatly expidite your support request.

Finally, option 99 will exit the SOS menu, returning you to a commnad shell.

Normally, each modification of the systems settings will cause the application to restart to make sure the Stratus application operates accordingly with the new settings. If this is not done, consider choosing option 4 to manually restart the application.

Service Packs installation is described in details in *Section C.3, "Software Upgrade"*.

C.5. Adding Storage

More Storage can be added to a system once it is already online, without requiring the system to be restarted. If the storage is already formatted, it can be added through the GUI interface, as described in *Section 3.4, "Manage Storage and Storage Consumers"*. If the storage is not formatted, this section will explain how to format the storage and add it to the system.

Note

This procedure requires a "shell" session on the Stratus server, either through a keyboard and monitor or through a remote shell application like SSH. It also requires "root" access to the Stratus server.

1. Log in to the system with 'root' privileged account, or as a less privileged account and switch to 'root' with the command **`su -`**.

2. Identify the unformatted storage volume's device name. One way to get this information is to run a command such as **`parted -l`** then search for the drive with no partition table. In the next examples, the device '/dev/sdd' will be used, but your device is likely to be different.

3. Identify what the new storage volumes ID will be. For a single-server system, sequential numbering should be fine. For a larger system, it may be worthwhile formulate a number convention to denote what physical disk (or disk group) each drive is, and to what server it is attached. For instance, va-3013 could mean "Server 3, channel 0, LUN 1, Partition 3. The 'va-' is required.

   In this example, the ID 'va-1234' will be used.

4. As 'root', run the command **`/opt/sarch/sm/sbin/sm_mkvolume /dev/sdd va-1234`**, remember to replace '/dev/sdd' with your device, and replace 'va-1234' with your drive ID.

5. After this, the storage is correctly formatted for best performance in Stratus. To add the newly formatted drive to available storage pool, use the Graphical Interface and refer to *Section 3.4, "Manage Storage and Storage Consumers"*.

C.6. Importing and Exporting CSV camera lists

You may wish to recreate system configuration with minimum hassle by exporting cameras into a CSV file and importing the CSV through the Add Camera Wizard.

First you will have to connect to system through ssh over "apl" account:

```
# ssh sos@192.168.xxx.xxx
```

Next, start SQL interpreter:

```
sos$ psql apl apl
```

Set postgres to export the next query to the home directory:

```
apl=# \o ~/cameras.csv
```

And execute next query:

```
apl=# select
md.val||','||id.val||','||ip.val||','||it.val||','||description||','
  ||location||','||us.val||','||pw.val
from _objs o
join _obj_attr id on id.obj=o.obj and id.attr='MODELID'
join _obj_attr md on md.obj=o.obj and md.attr='CAMERAMODEL'
join _obj_attr ip on ip.obj=o.obj and ip.attr='DEVIP'
join _obj_attr it on it.obj=o.obj and it.attr='CAMERA'
join _obj_attr us on us.obj=o.obj and us.attr='USRNAME'
join _obj_attr pw on pw.obj=o.obj and pw.attr='PASSWD'
where o.otype='D' and o.subtype='C' and o.deleted=0;
```

You will now have a csv file that you can import again in the Add Camera Wizard.

The format of the CSV file is:

'<Camera Make>,<Camera Model>,<IP Address>,<Channel (if present)>,<Description>,<Location>,<Username>,<Password>'

Appendix D. Device Support

D.1. Supported Video Cameras

Table D.1. Supported Cameras

Manufacturer	Model[s]	Supported features	Comments
ACTi	TCM/TCD series	Video: MJPEG/ H.264/ MPEG-4	Other cameras may be supported, but not tested
Arecont	all models	Video: MJPEG/ H.264/ MPEG-4	
Axis	all models	Video: MJPEG/ H.264/ MPEG-4; PTZ[1]; Motion Detection alerts	Firmware upgrade may be needed for older models
BAE Systems	LTC500		
Bosch	VIP-10/1000	Video: MJPEG; PTZ[2]	
Cisco	2500, 2500W		
Dante Security	SpeedDome	Video: MJPEG / H.264; PTZ	
FLIR	Nexxus enabled series	Video: MJPEG/ MPEG-4; PTZ[3]	
GrandEye	Halocam	Video: MJPEG; PTZ	Megapixel cameras with 360˚ fisheye lens and virtual PTZ
iQeye	Basic/Pro	Video: MJPEG; Motion Detection and Sensor Input for alerts	Megapixel cameras
Lumenera	LE series	Video: MJPEG	Megapixel cameras
Mango DSP	Raven-M	Video: MJPEG/ MPEG-4	
Panasonic	BB, WV series	Video: MJPEG/ MPEG-4; PTZ	
	WV-N series	H.264 video and audio	
Pelco	Spectra IV IP, Spectra miniDome	Video: MJPEG/ MPEG-4; PTZ	
Phoenix	IVS Intelligent Video Sensor	MJPEG / H.264 video	
QuickSet	QPT Series, Sentry Series, GeminiEye, QPT-LT		
Radiant	V4400	MPEG-2 video	
Samsung	SNC-5xx series	Video: MJPEG/ MPEG-4	

Manufacturer	Model[s]	Supported features	Comments
SightLogix	SightSensor	Video: MPEG-4	Megapixel cameras with Object Tracking
Sony	SNC, DF series	Video: MJPEG/ H.264/ MPEG-4; PTZ	
Toshiba	IK-WB series	Video: MJPEG	
UDP	NVC/NVE / IPEseries	Video: MJPEG/ MPEG-4/ H.264; PTZ	VCA Analytics
Verint	S19xx series	Video: MJPEG/ MPEG-4	
videoNEXT	VNE Series	MJPEG / H.264 video and audio	VCA Analytics
Vivotek		MJPEG / MPEG-4 / H.264 video	

Note

1. Stratus will support almost any type of camera PTZ with Axis-native loadable drivers. In addition (through Axis “Generic” driver and internal protocol implementation) Stratus supports ICD-TASS-001 compliant cameras: FLIR/MRTI/WSTI/COHU/..., QuickSet QPT/Sentry series (with FLIR Ranger or BAE LTC550 lens), QuickSet GeminiEye QPT-LT.
2. Bosch camera PTZ works through standard “Pelco” Stratus driver when PTZ Transport is set to “Bosch” to accommodate for Bosch's proprietary communications protocol
3. To support PTZ on FLIR cameras you have to have Nexus software enabled and configured properly. Stratus PTZ will work through Nexus API.

D.2. Supported Relay / Sensors

Table D.2. Supported Sensors / Relays

Manufacturer	Model[s]	Supported Features	Comments
Axis	All Models	Event Generation for Dry Contact trigger condition	Firmware upgrade may be needed on older models
Sony	SNC, DF series	Event Generation for dry contact trigger condition	
ACTi	SED-21XX series	Event Generation for dry contact trigger condition	
UDP	NVC Series	Event Generation for dry contact trigger condition, Relay output control	
videoNEXT	VNE series	Event Generation for dry contact trigger condition, relay output control	

Appendix E. Support

Customer Support

videoNEXT offers technical support to all customers to ensure smooth and effective operation.

Web Support:

Please go to *www.videonext.com* >Support >Technical Support> Select Option 1 or 2 and follow the prompts.

Telephone Support:

Dial Toll-free Number 1.866.723.3077 for calls within the USA

Dial +1.703.657.1200 for calls originating from other countries

Choose Option 1 for Sales or Option 2 for technical support

Please have your Product Serial Number ready when you contact us or include the information in your e-mail. Be as specific and clear as possible in explaining your question, concern, or need so we can respond appropriately.

Please visit *www.videoNEXT.com*[1].

[1] www.videonext.com

Appendix F. Release Notes Stratus 3.3

This document provides an outline of new features in the Stratus release 3.3. We encourage you to read the Stratus 3.3 Administrator Manual and the Stratus 3.3 User Manual for more details on how to use new capabilities effectively.

1. VCA analytics integrated into Stratus software.

   Stratus software now incorporates an analytics engine from VCA Technology directly in the software, opening the possibility to perform video-analytics processing even on the cameras not equipped with such an option by the hardware manufacturer. Stratus software includes all functionality required to easily deploy an integrated solution, enable and calibrate analytical engine and to define multiple behavioral rules to substantially reduce the need in continuous monitoring by the operator, resulting in productivity improvements.

   Rapid improvements in server CPU technologies from Intel and AMD makes this path more economical and better suited for long-term infrastructures maintenance and updates, resulting in longer usable solution life-span. This enables a cost-effective retrofitting for existent IP surveillance deployment as well as easier maintenance and expansion on newly-planed installs.

   This is a separately-licensed option for the Stratus product, please inquire our Sale Team (sales@videonext.com) for details on pricing and bundled packages.

2. Object Video analytics integrated into Stratus software.

   Stratus software now incorporates an analytics engine from ObjectVideo directly in the software, opening the possibility to perform video-analytics processing even on the cameras not equipped with such an option by the hardware manufacturer. Stratus software includes all functionality required to easily deploy an integrated solution, enable and calibrate analytical engine and to define multiple behavioral rules to substantially reduce the need in continuous monitoring by the operator, resulting in productivity improvements.

   Rapid improvements in server CPU technologies from Intel and AMD makes this path more economical and better suited for long-term infrastructures maintenance and updates, resulting in longer usable solution life-span. This enables a cost-effective retrofitting for existent IP surveillance deployment as well as easier maintenance and expansion on newly-planed installs.

   This is a separately-licensed option for the Stratus product, please inquire our Sale Team (sales@videonext.com) for details on pricing and bundled packages.

3. Extended system audit.

   The functionality of “Application Log” of prior Stratus software was completely replaced with brand-new implementation, which collects substantially more information about system operation, configuration changes and usage by Operators. The Audit Log provides a cross-searchable database, which is exposed via “Full Audit Log” and through multiple filters, which allow to review activities relevant to particular Device , User, Role, etc...

   All of this data is exposed in “Control Panel” user interface. In addition, the same audit log stores the history about Operators’ actions over Events, which is exposed in “Matrix” user interface for the Operators with “Supervisor” or higher permission level, that allows to keep track of the steps and actions taken by Operator[s] to review and clear alarm conditions.

4. Scheduler functionality refactored and expanded.

   The Scheduler became a system-wide set of Policies, which are established in one place (in the boundaries of Stratus Security Domain) and then are used by any camera device in the

system. This design consideration significantly simplifies system deployment and maintenance. The Schedule creation and modification process was simplified with scheduler user interface in the “Control Panel” similar to that of Google Calendar, which allows the user to define multiple individual and repeating time intervals and associated System Posture settings, which control the most important settings like Device State (on/off), Storage Policy, Motion Detection, etc...

The Schedule policy has the important concept of the Default Posture, which defines which individual setting[s] will be controlled by the Schedule and their default values. Once a Schedule is assigned to certain device, it takes over (overrides) listed parameters’ maintenance (in other words, old values of these settings on device have no effect after that and are disabled, since now schedule controls it). This allows for relative ease of system administration and maintenance, especially for installations with tens and hundreds of devices. (For more information, see *Section 4.11, “Schedule Manager”*).

5. New “STD: No Archive” Storage Policy.

   Previous versions of Stratus did not have a dedicated Storage policy to disable writing video to media archive (while it was quite easy to emulate with setting Motion Detection sensitivity to low level and using “Motion Only” storage policy). After introduction of revised/improved Schedule (see 1.4 above), a dedicated policy for “Live Only” policy became necessary for easier management in the situations where for example recording is not needed during certain periods of time, but which can not be covered with “STD: Motions Only” policy.

6. Newest browsers support with TibcoGI 3.9 engine update.

   Our upstream vendor issued a new runtime engine with better load speed and improved Internet Explorer 9, Safari 5 and FireFox 6 support. It is incorporated into Stratus 3.3 as a part of Stratus Support and Maintenance process. Runtime engine introduction into prior releases is not planned and we are encouraging our customers to utilize their free upgrade program to get benefits from runtime update and other new and improved features of Stratus 3.3.

7. MediaPlayer improvements for better video delivery.

   Stratus has alway been supporting popular browser working under both Windows and Mac OS X client platforms for real-time video/audio delivery. Previously it was relying on Java platform to enjoy this cross-platform portability, but this technologies carried a drawback of less-then-optimal system resource usage.

   Stratus release 3.3 introduces native browser plugins/helpers with better performance and more smooth video and audio playback capabilities. These software components are delivered to the client platforms automatically and transparently, so users do not experience any additional discomfort for installation/activation steps (same as it was done with previous components).

   In addition, new MediaPlayer components have “video enhancement” functionality built-in, which allows to adjust brightness and contrast (in addition to digital pan-tilt-zoom, which is a standard feature of prior software versions). To adjust any of these settings, a User would need to hover the mouse pointer over left-top corner of the video and wait the split-second for the icons for brightness / contrast / digital zoom to appear, select a mode to be adjusted and use mouse scroll wheel to change setting.

8. EventLog GUI improvements.

   Specifically:

   - The EventLog is an important “radiator of information” for multi-user Stratus installations and it received a number of updates in release 3.3. The “Event Details” modal dialog window was

completely reworked and changed into multi-tabbed component to provide screen real estate for more information and controls.

- All important read-only information was consolidated into bigger and better arranged “General info” tab, which opens first, so Operator may review the essence of alert quickly.
- An additional tab provides more space for Event Preview (snapshots over entire event with 5-seconds-pitch) on both Event Source device and on any Associated Witness devices
- An additional tab provides more space for the Operator to review the comments of other operators and to provide his(her) own comments
- Additional tab for Event Audit History
- Additional tab for device control (for example, associated Access Control devices)
- Another improvement to simplify Event Monitoring and to facilitate a separation of responsibilities in a multi-user installation is in the ability to add Event Priority into the "FILTER" of EventLog. Effectively this allows the user to ignore low-priority entries as needed.
- Another improvement to EventLog interface is to visually indicate that the "FILTER" is active, so that the Operator is aware that the Even-flow observed may be restricted because of the filter(s) that are applied.

9. CISCO VSOM integration.

   Stratus 3.3 adds “Cisco VSOM” as one of the video-input sources which is natively supported, so video may be ingested into Stratus source.

   Another function for this integration is to allow Stratus to push its events back to CISCO VSOM software using “Notification HTTP URL”, which may be used to trigger “soft-trigger” on CISCO's side, for example to push Events from VCA or ObjectVideo Video Analytics into CISCO VSOM (see 1.1 / 1.2 above).

10. Support for Cisco CIVS-IPC-4300 cameras.

    Support for Cisco CIVS-IPC-4300 cameras was added for all resolutions and codecs supported (MJPEG, H.264).

11. Support for Bosch NBC-255P / Bosch NWC-495.

    Support for Bosch NBC-255P and NWC-495 was added for all resolutions and codecs supported (MJPEG, H.264).

12. Support for MOXA video encoders.

    Support was added for video-retrieval from MOXA devices, MJPEG and H.264 codecs.

13. GEO-PTZ commands exposed to HTTP PTZ API.

    Previously, integrators needed to implement “MBus” interface to take advantage of “GEO-enabled PTZ” functionality. Now this functionality is exposed via less complex HTTP API. Please refer to API document for details. Consult your Sales Representative if you do not have API document access.

14. Stratus installation process refactoring.

Stratus release 3.3 was significantly improved internally for easier upgrades, which allows us to abandon the “Service Pack” type of maintenance starting from this release. As a part of this refactoring effort, installation and update process were modified to include a distinct “activation” step to facilitate the “update in place” scenario with easy customer data migration between subsequent software Major and Minor Releases. This will allow videoNEXT to serve our customer better and to reduce time to deliver changes and fixes. Please refer to the “Installation Guide” document for more details.

15. Software Security improvements.

    Stratus 3.3 is supplied with installation procedure suitable for deployment in various level of secured environments: starting from “unsecured” (level=0) to “DOD secured” (level=2). A set of extensive security scans and reviews was performed on the consolidated OS+software solution to ensure substantially improved level of protection to the deployed system. Please consult with your Sales Representative about the current security approval ratings and certifications on the Stratus product and relevant bundles.

16. “Reports” removed from “Control Panel” (Admin) GUI.

    As a part of “Software Security improvements” (see 15 above), “Report” menu item was removed from the “Control Panel” (Admin) GUI due to potential vulnerabilities and/or lack of security approvals on third-party software components previously utilized. As an alternative, videoNEXT suggests to utilize a standard external monitoring systems like HP OpenView or free/open-source alternatives.

    This Wikipedia link may be a good starting point:*http://en.wikipedia.org/wiki/Network_monitoring_comparison*

17. Streamlined OEM/branding process.

    videoNEXT can support integrators / resellers with specific OEM-branded software release and bundles, where product name, logos, and contact information will be substituted with selected brand easily in current and any subsequent produce versions. Please consult with your Sales Representative about the details.

18. Platforms support

    Stratus 3.3 server side requires the RedHat Enterprise Linux 5.7 32-bit Operating System to operate. CentOS may be used as a replacement with no commercial OS support.

    Selecting kernel with PAE support is strongly recommended and is default for supplied kick-start-based installation procedure.

    The Server should have at least 2 GB of RAM and a dedicated physical OS/software disk (not shared with video-archive disks). 4GB of RAM is strongly recommended, while 8GB is the ideal size for highly-loaded system (with tens of high-resolution cameras). Installing more than 8GB of RAM is possible, but is not recommended since the OS and application would not be able to use it effectively.

    Hardware platforms supported include leading vendors like DELL and HP and should be selected to support RedHat Enterprise Linux 5 / 32 bit. Please inquire for list of currently certified hardware solutions from support@videonext.com.

    videoNEXT supplies a kick-start install scripting file, which must be used to get the proper environment created on the server side. Warranty claims relevant to installations done with an environment not certified by videoNEXT will not be honored.

On the client side, Microsoft Internet Explorer 7/8/9 and Google Chrome are supported for web-clients accessing the Stratus system. Apple MAC OS X platforms include Snow Leopard (v10.6.2+) and Lion (10.7.1+) with Safari 5.0.x or FireFox browsers.

Note

Apple's Safari 5.1.0 browser has a known bug in Java Plugin, which leads to an intermittent problems with some Mac OS X systems. videoNEXT recommends to postpone installing update to Safari 5.1.0 or to use FireFox in place of Safari on Mac OS X client computers.

19. General notes

General note of caution: avoid using special character like ‘#’ '<', '>', '&', '\', "', "" in the device names, saved configuration names, policy names, etc.. It potentially could break some of the functionality. As a first troubleshooting step, try removing these special characters from the names and see if your problem is resolved. Please submit your findings to support@videonext.com and reported defects will be accommodated in the next product release.

Appendix G. Revision History

Revision 0-0 **Tue Jul 5 2011** **Jeffrey Scott** *jeff.scott@videonext.com*

Initial creation of book by publican

Revision 0-1 **Tue Jul 21 2011** **Jeffrey Scott** *jeff.scott@videonext.com*

Added section id's
Added internal references

Revision 1-0 **Tue Sept 12 2011** **Jeffrey Scott** *jeff.scott@videonext.com*

Revisions provided by George.

Revision 1-1 **Tue Nov 23 2011** **Jeffrey Scott** *jeff.scott@videonext.com*

Updates to 3.3 release version.

Revision 1-2 **Tue Jan 11 2012** **Jeffrey Scott** *jeff.scott@videonext.com*

Minor language fixes.